ProCurve MSM7xx Controllers

Management and Configuration Guide

HP ProCurve MSM7xx Controllers

Management and Configuration Guide

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

This guide contains proprietary information, which is protected by copyright. No part of this guide may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard.

Publication Number

5992-5929
May 2009

Applicable Products

MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
MSM730 Access Controller	J9329A
MSM730 Mobility Controller	J9326A
MSM750 Access Controller	J9330A
MSM750 Mobility Controller	J9327A
MSM760 Access Controller	J9421A
MSM760 Mobility Controller	J9420A
MSM765zl Mobility Controller	J9370A

	USA part	WW part
MSM310 Access Point	J9374A	J9379A
MSM310-R Access Point	J9380A	J9383A
MSM317 Access Device	J9422A	J9423A
MSM320 Access Point	J9360A	J9364A
MSM320-R Access Point	J9365A	J9368A
MSM325 Access Point with Sensor	J9369A	J9373A
MSM335 Access Point with Sensor	J9356A	J9357A
MSM410 Access Point	J9426A	J9427A
MSM422 Access Point	J9358A	J9359A

Trademark Credits

Windows NT®, Windows®, and MS Windows® are US registered trademarks of Microsoft Corporation.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Open Source Software Acknowledgement Statement

This software incorporates open source components that are governed by the GNU General Public License (GPL), version 2. In accordance with this license, HP ProCurve Networking will make available a complete, machine-readable copy of the source code components covered by the GNU GPL upon receipt of a written request. Send a request to:

Hewlett-Packard Company, L.P.

GNU GPL Source Code

Attn: ProCurve Networking Support

Roseville, CA 95747 USA

Safety and regulatory information

Before installing and operating this product, please read

- *Safety information on page 1-9.*
- *Appendix A: Safety and EMC regulatory statements*

Hewlett-Packard Company
8000 Foothills Boulevard
Roseville, California 95747-5552
www.procurve.com

Contents

1 Introduction

About this guide 1-2
- Products covered 1-2
- HP ProCurve Networking product naming 1-3
- Important terms 1-4
- Conventions 1-4

New in this release 1-6

Introducing the MSM7xx Controllers 1-7
- Simplified configuration, deployment, and operation 1-8
- Seamless mobility 1-8
- Best-in-class public/guest network access service 1-8

Safety information 1-9

HP ProCurve Networking support 1-10

Getting started 1-10

Online documentation 1-10

2 Working with VSCs

Key concepts 2-3
- Viewing and editing VSC profiles 2-4
- The default VSC 2-4

VSC configuration options 2-5
- About access control and authentication 2-6
- Summary of VSC configuration options 2-8
- Access control 2-9
- Virtual AP 2-9
- VSC ingress mapping 2-11
- VSC egress mapping 2-11
- Default user data rates 2-12
- Wireless mobility 2-12
- Wireless security filters 2-13
- Wireless protection 2-13

802.1X....2-16
RADIUS authentication realms....2-16
HTML-based user logins....2-17
VPN-based authentication....2-18
MAC-based authentication....2-18
Location-aware....2-19
Wireless MAC filter....2-19
Wireless IP filter....2-20
DHCP server....2-20
DHCP relay agent....2-20
VSC data flow....2-21
Access control enabled....2-22
Access control disabled....2-23
Using multiple VSCs....2-24
About the default VSC....2-25
Quality of service (QoS)....2-25
Priority mechanisms....2-26
IP QoS profiles....2-28
Upstream DiffServ tagging....2-29
Upstream/downstream traffic marking....2-29
QoS example....2-31
Creating a new VSC....2-32
Assigning a VSC to a group....2-32

3 Working with controlled APs

Key concepts....3-3
Key controlled-mode events....3-5
Discovery of controlled APs....3-7
Discovery overview....3-7
Discovery methods....3-8
Discovery recommendations....3-9
Discovery priority....3-10
Discovery behavior....3-11
Discovery considerations....3-12

Monitoring the discovery process 3-13

Authentication of controlled APs 3-18
Building the AP authentication list 3-18

Configuring APs 3-21
Overview 3-21
Configuration strategy 3-23
Working with groups 3-23
Working with APs 3-25

Defining VLANs 3-28

Provisioning 3-31
Provisioning methods 3-31
Displaying the provisioning pages 3-32
Provisioning connectivity 3-34
Provisioning discovery 3-36
Provisioning summary 3-37

AeroScout RTLS 3-38

Software retrieval/update 3-39

Monitoring 3-39

4 Management

Management tool 4-2
Management scenarios 4-2
Management station 4-2
Starting the management tool 4-2
Customizing management tool settings 4-3
Security policies 4-6
Security 4-6
Web server 4-7
Auto-refresh 4-7

Device discovery 4-8
Mobility controller discovery 4-8
Controlled AP discovery 4-9

SNMP 4-10
Configuring the SNMP agent 4-10

SOAP 4-13
Configuring the SOAP server 4-13
CLI 4-15
Configuring CLI support 4-15
System time 4-16
Country 4-17

5 Security

Overview 5-2
Firewall 5-2
Firewall presets 5-3
Firewall configuration 5-4
Customizing the firewall 5-5
Managing certificates 5-6
Trusted CA certificate store 5-6
Certificate and private key store 5-9
Certificate usage 5-10
About certificate warnings 5-11
IPSec certificates 5-12

6 Authentication services

Overview 6-2
Using the integrated RADIUS server 6-2
Server configuration 6-3
User account configuration 6-4
Using a third-party RADIUS server 6-5
Configuring a RADIUS server profile on the service controller 6-5
Using an Active Directory server 6-9
Active Directory configuration 6-9
Configuring an Active Directory group 6-12
Configuring a VSC to use Active Directory 6-14

Configuring global 802.1X settings....6-15
Configuring MAC lists....6-15

7 User authentication

Key concepts....7-2
Authentication support on a service controller....7-2
Authentication support on a controlled AP....7-2
Authentication types....7-3
Locally-defined user accounts....7-5
Features....7-5
Defining a user account....7-9
Defining account profiles....7-11
Defining subscription plans....7-13
Accounting persistence....7-14

8 Public/guest network access

Key concepts....8-3
About the public and protected networks....8-3
About the public access interface....8-4
Public access examples....8-4
Default configuration....8-4
Public access interface tour....8-5
About the “Subscribe to the service” feature....8-5
About the “Use Free Access service” feature....8-8
About the “Existing user” feature....8-8
Displaying advertisements....8-10
Public access interface flow....8-11
Customizing the public access interface....8-12
Common configuration tasks....8-13
Setting site configuration options....8-18
Allow subscription plan purchases....8-18
Display the Free Access option....8-19
Support a local Welcome page....8-19
Use frames when presenting ads....8-19

Allow SSLv2 authentication 8-20
Redirect users to the Login page via 8-20
Customizing public access interface Web pages 8-21
Site file archive 8-21
FTP server 8-21
Current site files 8-22
Global access control settings 8-29
Access control parameter definitions 8-30
Web server configuration 8-33
Options 8-33
Ports 8-34
MIME types 8-34
Security 8-35
Payment services 8-36
Payment services configuration 8-36
Service settings 8-36
Billing record logging 8-38
Settings 8-39
Persistence 8-40
External billing records server profiles 8-40
Billing records log 8-43
Location-aware authentication 8-45
How it works 8-45
Example 8-47
Security 8-48

9 Working with public access attributes

Defining and retrieving site attributes 9-3
Retrieve attributes using RADIUS 9-3
Configured attributes 9-4
Defining and retrieving user attributes 9-5
Defining attributes locally in user accounts 9-5
Retrieving attributes from a RADIUS server 9-9

Attribute definitions....9-10
Site attributes....9-11
User attributes....9-17
Administrator attributes....9-27

Colubris AV-Pair attribute - Site values....9-29
Access list....9-30
Configuration file....9-41
Custom SSL certificate....9-41
Custom public access interface Web pages....9-42
Default user interim accounting update interval....9-48
Default user bandwidth level....9-49
Default user idle timeout....9-49
Default user quotas....9-49
Default user data rates....9-50
Default user one-to-one NAT....9-50
Default user session timeout....9-51
Default user public IP address....9-51
Default user SMTP server....9-51
Default user URLs....9-52
HTTP proxy upstream....9-52
IPass login URL....9-53
MAC authentication....9-53
Multiple login servers....9-54
Redirect URL....9-56
NOC authentication....9-59
ProCurve WISPr support....9-59
Traffic forwarding (dnat-server)....9-60
Multiple DNAT servers....9-61

Colubris AV-Pair attribute - User values....9-63
Access list....9-64
Advertising....9-65
Bandwidth level....9-65
Data rate....9-65
One-to-one NAT....9-66
Public IP address....9-66
Quotas....9-66
Redirect URL....9-67
SMTP redirection....9-67

Station polling 9-68
Colubris AV-Pair attribute - Administrator values 9-69
Administrative role 9-69
Public access interface ASP functions and variables 9-70
Javascript syntax 9-71
Forms 9-71
Form errors 9-74
RADIUS 9-75
Page URLs 9-76
Session status and properties 9-77
iPass support 9-81
Web 9-83
Client information 9-83
Subscription plan information 9-85
Other 9-86
Session information 9-89

10 Network configuration

Port configuration 10-3
LAN port configuration 10-4
Internet port configuration 10-5
Address allocation 10-6
DHCP server (global) 10-6
DHCP relay agent 10-9
VLAN support 10-11
Types of VLANs 10-11
VLAN configuration 10-12
GRE tunnels 10-14
Bandwidth control 10-15
Internet port data rate limits 10-16
Bandwidth levels 10-16
Example 10-17

CDP 10-18

DNS 10-19
DNS servers 10-19
DNS advanced settings 10-20

IP routes 10-21
Configuration 10-21

Network address translation (NAT) 10-23
NAT security and static mappings 10-24
VPN One-to-one NAT 10-26

RIP 10-27

IP QoS 10-27
Configuration 10-28
Example 10-29

IGMP proxy 10-31

11 Wireless mobility

Mobility license 11-2

Key concepts 11-2
WPA2 Opportunistic key caching 11-2
Layer 3 Mobility 11-3

Wireless mobility scenario 11-3

12 Working with VPNs

Overview 12-2

Securing wireless client sessions with VPNs 12-3
Configure an IPSec profile for wireless client VPN 12-4
Configure L2TP server for wireless client VPN 12-5
Configure PPTP server for wireless client VPN 12-5
VPN address pool 12-6

Securing service controller communications to remote VPN servers 12-7
Configure an IPSec policy for a remote VPN server 12-8
Configure PPTP client for a remote VPN server 12-9

Keeping user traffic out of the VPN tunnel 12-11

Additional IPSec configuration 12-11
IPSec VLAN mapping 12-12
Local group list 12-12
IPSec security policy database 12-12

13 Local mesh

Introduction 13-2

Local mesh terminology 13-3

Local mesh operational modes 13-4

Node discovery 13-4

Operating channel 13-5

Local mesh profiles 13-5
Configuration guidelines 13-6
Configuring a standard profile 13-7
Other configuration settings 13-9

Provisioning local mesh links 13-12

Sample local mesh deployments 13-15
RF extension 13-15
Building-to-building connection 13-15
Dynamic network 13-16

14 Working with autonomous APs

Key concepts 14-2
Autonomous AP detection 14-3
Viewing autonomous AP information 14-3
Switching a controlled AP to autonomous mode 14-4

Configuring autonomous APs 14-4
VSC definitions 14-5

Working with third-party autonomous APs 14-6
VSC selection 14-6

15 Maintenance

Config file management 15-2
Manual configuration file management 15-2
Scheduled operations 15-3

Software updates 15-5
Performing an immediate software update 15-5
Performing a scheduled software update 15-6

Managing licenses 15-7
Factory installed licenses 15-7
User installed licenses 15-7
License management 15-8
Factory reset considerations 15-8

A Safety and EMC regulatory statements

Safety Information A-2

Informations concernant la sécurité A-2

Hinweise zur Sicherheit A-3

Considerazioni sulla sicurezza A-4

Consideraciones sobre seguridad A-5

Safety Information (Japan) A-6

Safety Information (China) A-7

EMC Regulatory Statements A-8
U.S.A. A-8
Japan A-8

Recycle Statements A-10
Waste Electrical and Electronic Equipment (WEEE) Statements A-10

B Console ports

Overview B-2
MSM710 Console port B-2
MSM730 Console port B-2
MSM750 Console port B-3

C Resetting to factory defaults

How it works C-2
Using the Reset button C-2
Using the management tool C-2
Using the Console (serial) port C-3

D NOC authentication

Main benefits D-2
How it works D-2
Activating a remote login page with NOC authentication D-4
Addressing security concerns D-5
Securing the remote login page D-5
Authenticating with the login application D-6
Authenticating the service controller D-6
NOC authentication list D-6
Setting up the certificates D-6
Install certificates on the Web server D-7
Define attributes D-7
Install a certificate on service controller D-7
Authenticating users D-8
Returned values D-9
Examples of returned HTML code D-11
Simple NOC authentication example D-12
Forcing user logouts D-13

E DHCP servers and Colubris vendor classes

Overview E-2
Windows Server 2003 configuration E-2
ISC DHCP server configuration E-7

1

Introduction

Contents

About this guide 1-2
- Products covered 1-2
- HP ProCurve Networking product naming 1-3
- Important terms 1-4
- Conventions 1-4

New in this release 1-6

Introducing the MSM7xx Controllers 1-7
- Simplified configuration, deployment, and operation 1-8
- Seamless mobility 1-8
- Best-in-class public/guest network access service 1-8

Safety information 1-9

HP ProCurve Networking support 1-10

Getting started 1-10

Online documentation 1-10

About this guide

This guide explains how to configure, and operate the MSM7xx Controllers. It also provides controlled-mode information for MSM3xx and MSM4xx Access Points and the MSM317 Access Device. For information on the operation of access points that support autonomous mode, see the *MSM3xx/MSM4xx Access Points Management and Configuration Guide*.

Products covered

This guide applies to the following MSM7xx Controller products:

Model	Part
MSM710 Access Controller	J9328A
MSM710 Mobility Controller	J9325A
MSM730 Access Controller	J9329A
MSM730 Mobility Controller	J9326A
MSM750 Access Controller	J9330A
MSM750 Mobility Controller	J9327A
MSM760 Access Controller	J9421A
MSM760 Mobility Controller	J9420A
MSM765zl Mobility Controller	J9370A

This guide provides controlled-mode information for the following MSM3xx and MSM4xx Access Points and the MSM317 Access Device ("USA" identifies USA versions, "WW" identifies worldwide versions for the rest of the world):

Model	USA part	WW part
MSM310 Access Point	J9374A	J9379A
MSM310-R Access Point	J9380A	J9383A
MSM317 Access Device	J9422A	J9423A
MSM320 Access Point	J9360A	J9364A
MSM320-R Access Point	J9365A	J9368A
MSM325 Access Point with Sensor	J9369A	J9373A
MSM335 Access Point with Sensor	J9356A	J9357A
MSM410 Access Point	J9426A	J9427A
MSM422 Access Point	J9358A	J9359A

HP ProCurve Networking product naming

As of October 1st, 2008, Colubris Networks was acquired by HP ProCurve Networking. HP ProCurve Networking has integrated the Colubris product line into its Networking product portfolio (**www.procurve.com/news/colubris-10-01-08.htm**).

In the online help and this manual, Colubris product names have been changed to their equivalent HP ProCurve Networking product names.

Note

SOAP and SNMP MIBs retain the Colubris naming so you do not need to change your existing SOAP and MIB usage.

The Colubris Networks product names and their corresponding new HP ProCurve Networking product names are as follows:

Colubris name	HP ProCurve Networking name
MSC-5100 MultiService Controller	MSM710 Controller
MSC-5200 MultiService Controller	MSM730 Controller
MSC-5500 MultiService Controller	MSM750 Controller
MAP-320 MultiService Access Point	MSM310 Access Point
MAP-320R MultiService Access Point	MSM310-R Access Point
MAP-330 MultiService Access Point	MSM320 Access Point
MAP-330R MultiService Access Point	MSM320-R Access Point
MAP-330 AP+Sensor MultiService Access Point	MSM325 Access Point with Sensor
MAP-625 MultiService Access Point	MSM422 Access Point
MAP-630 AP+Sensor MultiService Access Point	MSM335 Access Point with Sensor
WCB-200 Wireless Client Bridge	M111 Client Bridge
Visitor Management Tool	Guest Management Software
RF Manager 1500 Enterprise	RF Manager 100 IDS/IPS system
RF Manager 1300 Basic	RF Manager 50 IDS/IPS system
RF Planner	RF Planner

Important terms

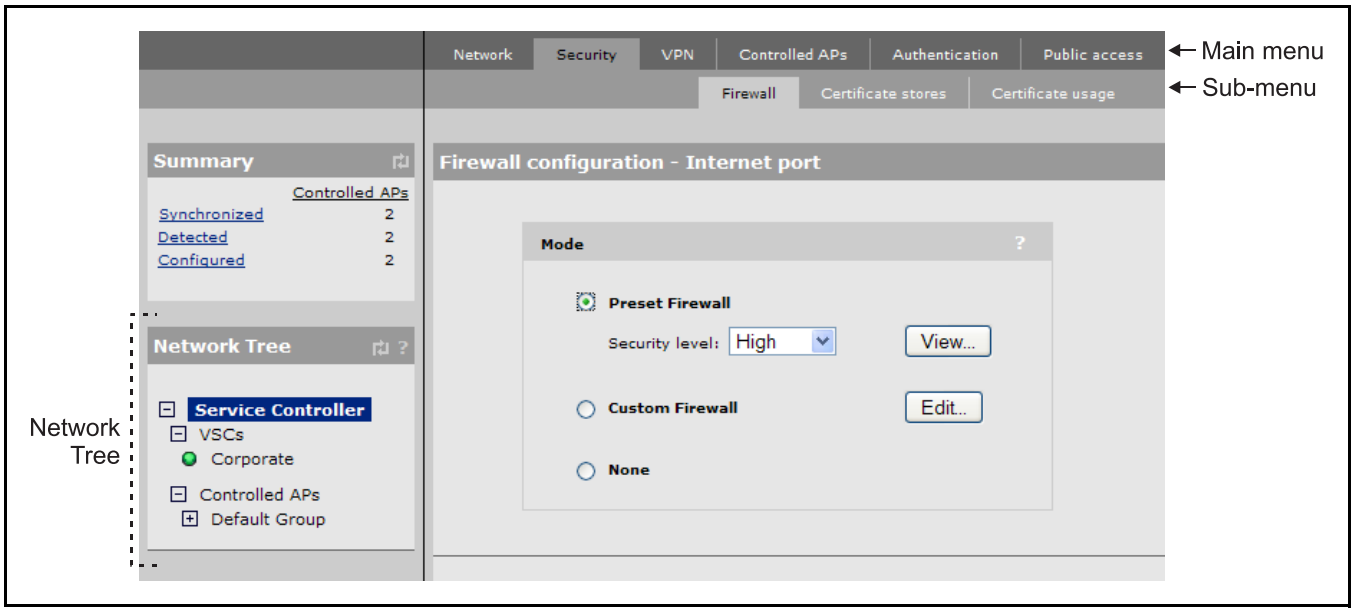
The following terms are used in this guide.

Term	Description
AP	Refers to any HP ProCurve Networking MSM3xx or MSM4xx Access Point or the MSM317 Access Device which is an Access Point with integrated Ethernet switch. Specific model references are used where appropriate. Non-HP ProCurve access points are identified as *third-party APs*. These APs do not support controlled-mode operation.
service controller	Refers to any HP ProCurve Networking MSM7xx Controller, including both Access Controller and Mobility Controller variants.

Conventions

Management tool

This guide uses specific syntax when directing you to interact with the management tool user interface. Key user-interface elements are identified as follows:



Example directions in this guide	What to do in the user interface
Select **Service Controller >> Security > Firewall**.	In the Network Tree select the **Service Controller** element, then on the main menu select **Security,** and then select **Firewall** on the sub-menu. All elements to the left of the double angle brackets **>>** are found in the Network Tree.

Example directions in this guide	What to do in the user interface
Select **Service Controller > VSCs >** [VSC name] **>> Configuration**.	Expand the **Service Controller** branch (click its **+** symbol), expand the **VSCs** branch, select a [VSC name], and select **Configuration** on the main menu.
For **Password** specify **secret22**.	In the **Password** field enter the text **secret22** exactly as shown.

Warnings and cautions

Do not proceed beyond a WARNING or CAUTION notice until you fully understand the hazardous conditions and have taken appropriate steps.

Warning Identifies a hazard that can cause physical injury or death.

Caution Identifies a hazard that can cause the loss of data or configuration information, create a non-compliant condition, or hardware damage.

Commands and program listings

Monospaced text identifies commands and program listings as follows:

Example	Description
`use-access-list`	Command name. Specify it as shown.
`ip_address`	Items in italics are parameters for which you must supply a value.
`ssl-certificate=`*`URL`* `[%s]`	Items enclosed in square brackets are optional. You can either include them or not. Do not include the brackets. In this example you can either include the "%s" or omit it.
`[ONE | TWO]`	Items separated by a vertical line indicate a choice. Specify only one of the items. Do not include the vertical line.

New in this release

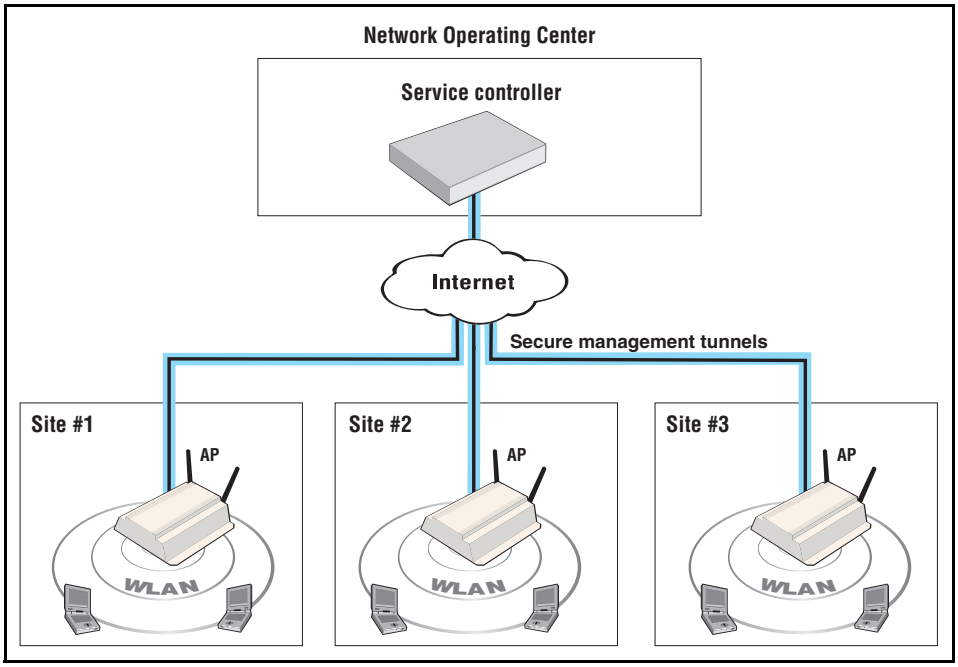
The following new features and enhancements have been added in releases 5.3.x:

New feature or enhancement	For information see...
Support for MSM760 Mobility Controller and MSM760 Access Controller.	This guide and also the *MSM760 Controllers Installation and Getting Started Guide*.
Support for MSM765zl Mobility Controller.	This guide and also the *MSM760 Controllers Installation and Getting Started Guide*.
Support for MSM317 Access Device	This guide and also the *MSM317 Access Device Installation and Getting Started Guide*.
Payment services and Billing record logging.	*Payment services on page 8-36* and *Billing record logging on page 8-38*.
Subscription plan enhancements, including additional quotas, ad-free service, billing service, and currency.	*Defining subscription plans on page 7-13* and *Defining a subscription plan for access purchase on page 8-8*.
Support for AeroScout Real-Time Location Tracking System (RTLS).	*AeroScout RTLS on page 3-38*.
Portal pages enhancements, including substantially-enhanced built-in web server and ftp server capability.	*Public access interface tour on page 8-5*.
Public IP addresses for wireless users (IP Upsell).	*Public IP address on page 7-14*.
The client data tunnel can now traverse NAT-enabled routers.	*Client data tunnel on page 2-10*.
Administrative roles: Both Manager and Operator users.	*Customizing management tool settings on page 4-3*.
Automatic user HTML authentication (Welcome Back).	*Public access interface tour on page 8-5*.
Support for RF Manager 5.5 and related security sensors.	The separate RF Manager 5.5 documentation.
Support for Simple Network Management Protocol (SNMP) v3.	*SNMP on page 4-10*.
Secure Traffic Tunneling.	*Terminate WPA at the service controller on page 2-14* and *Securing wireless client sessions with VPNs on page 12-3*.
Fixed IP address leases on DHCP server.	*Active fixed leases on page 10-8*.
Support for three DNS servers	*DNS servers on page 10-19*.

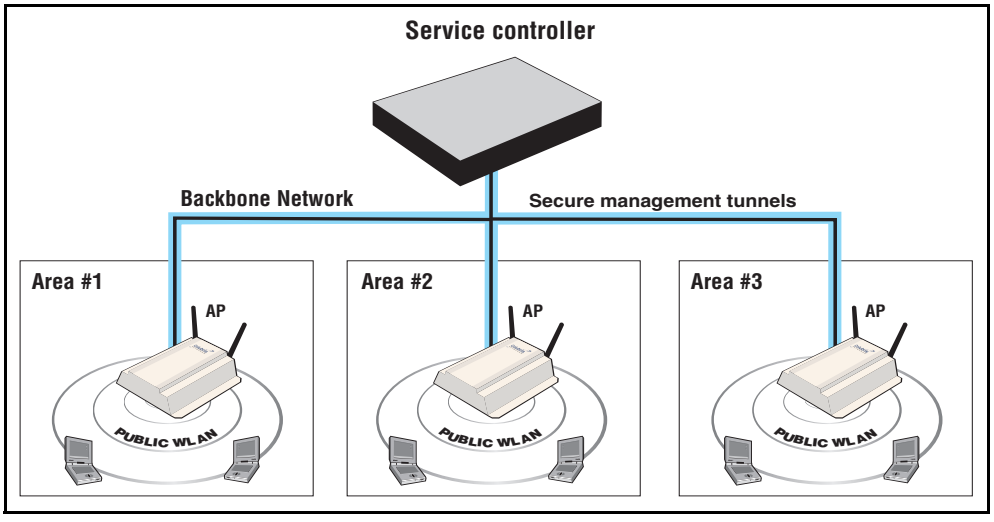
Introducing the MSM7xx Controllers

The HP ProCurve Networking MSM7xx Controllers provide centralized management and control of intelligent HP ProCurve Networking MSM APs distributed throughout a wireless zone, building, or campus, without the penalty of centralized switching. This significantly reduces backbone loads since user traffic is switched at the network edge and flows directly from source to destination. Service controllers handle only network control, management information, public access interface, and some authentication tasks, making them highly-scalable, cost-effective solutions.

Service controller managing APs installed in different physical locations



Service controller managing APs installed in different areas at a location



Simplified configuration, deployment, and operation

For trouble-free deployment in geographically distributed networks, HP ProCurve Networking MSM service controllers automate discovery, authentication and configuration for a group of APs. Using standard dynamic look-up procedures, APs identify the service controller to which they are assigned. Mutual authentication using digital certificates assures security and eliminates the risk of rogue AP connectivity. Once authenticated, the service controller establishes a secure management tunnel for the exchange of configuration and control information with the AP.

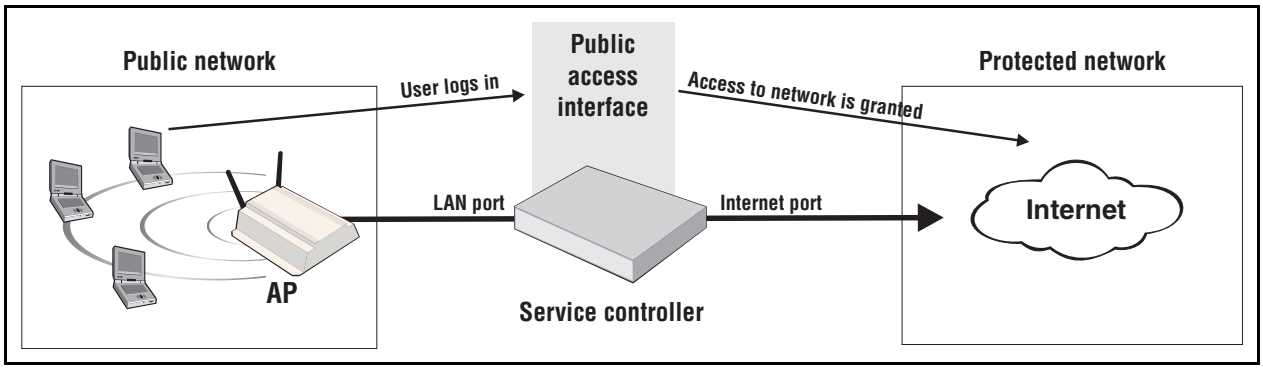
The service controller provides centralized management for all APs. It eliminates time-consuming AP configuration, troubleshooting and maintenance tasks by providing a single management interface for the entire group of APs it manages. The service controller automates installation of AP software updates and ensures a consistent set of services are delivered throughout the network. All security, quality of service (QoS), and other policies can be centrally defined through the service controller's intuitive and secure Web-based management tool.

Seamless mobility

MSM service controllers include basic L2 (Layer 2) mobility support allowing wireless users to roam between MSM APs within the same subnet. The optional Mobility license enhances basic wireless mobility by adding two separate features, WPA2 Opportunistic Key Caching and L3 Mobility.

Best-in-class public/guest network access service

Designed to deliver the best possible user experience, the public/guest network access feature adapts to any client device IP address and Web proxy settings, and provides a customizable Web login page for easy sign-on.



To ensure seamless applications support, the public/guest network access feature uses advanced IP networking capabilities, SMTP redirect, and DHCP services, providing transparent support for demanding applications, such as VPN tunneling and email.

A rich feature set allows service providers to create a centrally-managed hotspot network. Support for a captive portal enables users to access Web content.

Safety information

Warning

Professional Installation Required

Prior to installing or using an service controller, consult with a professional installer trained in RF installation and knowledgeable in local regulations including building and wiring codes, safety, channel, power, indoor/outdoor restrictions, and license requirements for the intended country. It is the responsibility of the end user to ensure that installation and use comply with local safety and radio regulations.

Cabling: You must use the appropriate cables, and where applicable, surge protection, for your given region. For compliance with EN55022 Class-B emissions requirements use shielded Ethernet cables.

Country of use: In some regions, you are prompted to select the country of use during setup. Once the country has been set, the service controller will automatically limit the available wireless channels, ensuring compliant operation in the selected country. Entering the incorrect country may result in illegal operation and may cause harmful interference to other systems.

Safety: Take note of the following safety information during installation:

- If your network covers an area served by more than one power distribution system, be sure all safety grounds are securely interconnected.
- Network cables may occasionally be subject to hazardous transient voltages (caused by lightning or disturbances in the electrical power grid).
- Handle exposed metal components of the network with caution.
- The MSM7xx Controller and all interconnected equipment must be installed indoors within the same building (except for outdoor models / antennas), including all PoE-powered network connections as described by Environment A of the IEEE 802.3af standard.

Servicing

There are no user-serviceable parts inside HP ProCurve Networking products. Any servicing, adjustment, maintenance, or repair must be performed only by trained service personnel.

HP ProCurve Networking support

HP ProCurve Networking offers support 24 hours a day, seven days a week through a number of automated electronic services. See the Customer Support/Warranty booklet included with your product. The HP ProCurve Networking Web site, **www.procurve.com/customercare** provides up-to-date support information. Additionally, your HP-authorized network reseller can provide you with assistance, both with services that they offer and with services offered by HP.

Before contacting support

To make the support process most efficient, before calling your networking dealer or HP Support, you first should collect the following information:

Collect this information	Where to find it
Product identification.	On the rear of the product.
Software version.	The product management tool **Login** page.
Network topology map, including the addresses assigned to all relevant devices.	Your network administrator.

Getting started

Get started by following the directions in the relevant guide as follows:

Product	Guide to use
MSM710, MSM730, MSM750	The provided *Quickstart*.
MSM760, MSM765zl	The provided *Installation and Getting Started Guide*.

Then continue with the next chapter of this guide.

Online documentation

For the latest documentation, visit the HP ProCurve Networking manuals Web page at: **www.procurve.com/manuals**.

Note

The MSM317 Access Device consists of both a controlled-mode-only access point and an integrated Ethernet switch. Where appropriate, this guide makes reference to the *MSM317 Installation and Getting Started Guide* which must be used in conjunction with this guide when working with the MSM317.

2

Working with VSCs

Contents

Key concepts....2-3
- Viewing and editing VSC profiles....2-4
- The default VSC....2-4

VSC configuration options....2-5
- About access control and authentication....2-6
- Summary of VSC configuration options....2-8
- Access control....2-9
- Virtual AP....2-9
- VSC ingress mapping....2-11
- VSC egress mapping....2-11
- Default user data rates....2-12
- Wireless mobility....2-12
- Wireless security filters....2-13
- Wireless protection....2-13
- 802.1X....2-16
- RADIUS authentication realms....2-16
- HTML-based user logins....2-17
- VPN-based authentication....2-18
- MAC-based authentication....2-18
- Location-aware....2-19
- Wireless MAC filter....2-19
- Wireless IP filter....2-20
- DHCP server....2-20
- DHCP relay agent....2-20

VSC data flow....2-21
- Access control enabled....2-22
- Access control disabled....2-23

Using multiple VSCs....2-24

About the default VSC....2-25

Quality of service (QoS)....2-25
- Priority mechanisms....2-26
- IP QoS profiles....2-28
- Upstream DiffServ tagging....2-29
- Upstream/downstream traffic marking....2-29
- QoS example....2-31

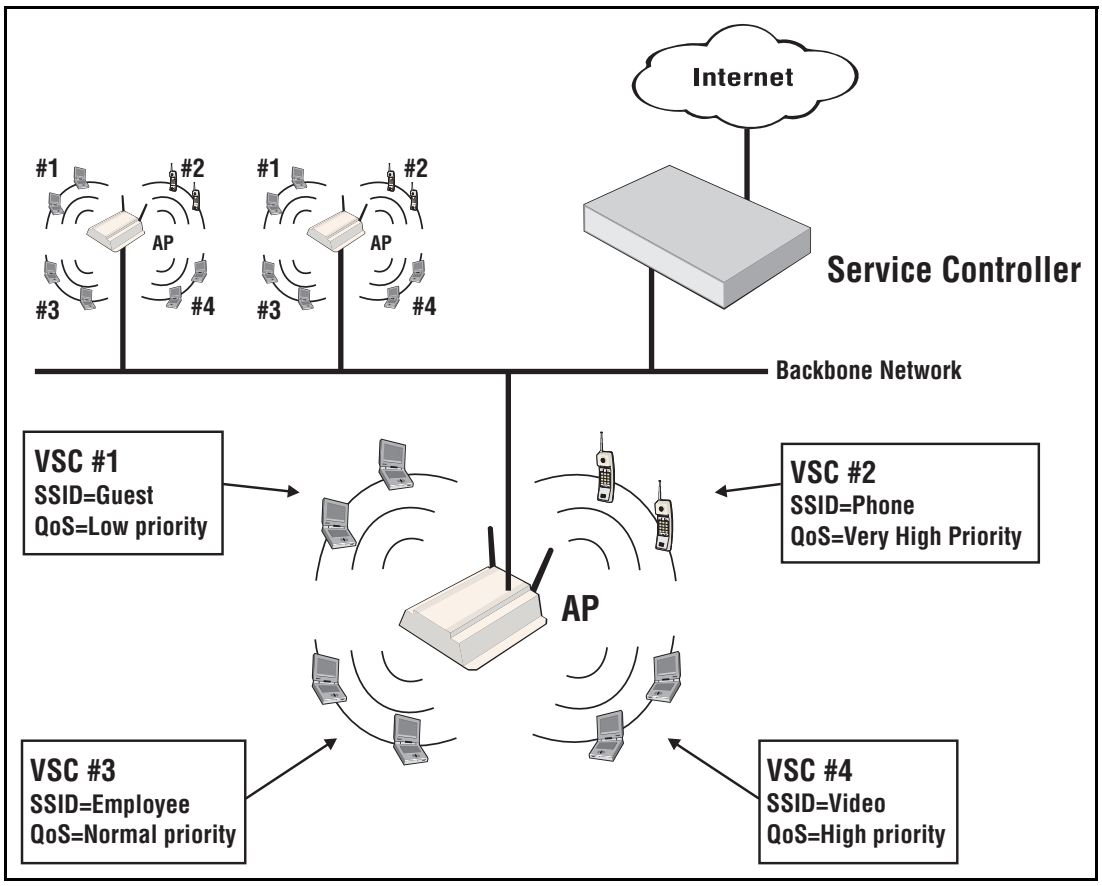
Creating a new VSC....2-32

Assigning a VSC to a group....2-32

Key concepts

A VSC (virtual service community) is a collection of configuration settings that define key operating characteristics of the service controller and controlled APs. In most cases, a VSC is used to define the characteristics of a wireless network.

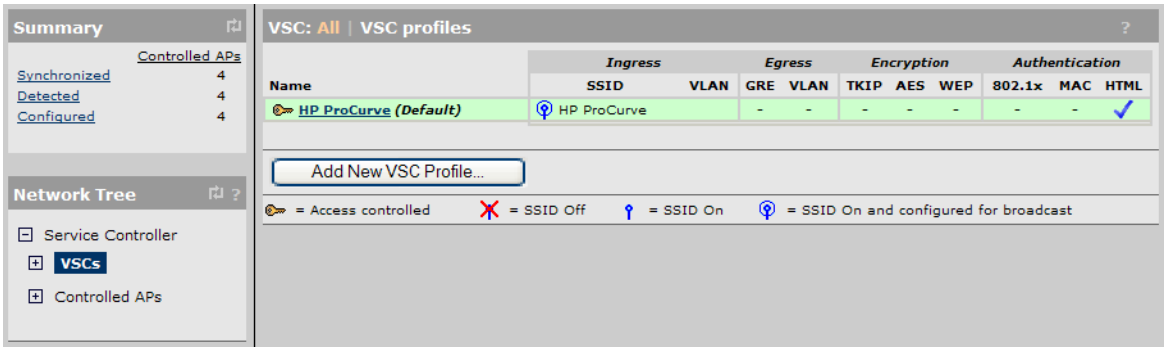
A service controller supports up to sixteen VSC profiles, allowing for great flexibility in the configuration of services. For example, in the following scenario four VSCs are used to support different types of wireless users. Each VSC is configured with a different wireless network name (SSID), and the quality of service (QoS) feature is used to classify user traffic priority.



The service controller defines a global pool of VSC profiles that represent the services that are available on the network. From this pool, specific VSC profiles can be *bound* to one or more groups (and the APs in the groups), to provide a homogeneous wireless offering. See *Binding VSCs to groups on page 3-22*.

Viewing and editing VSC profiles

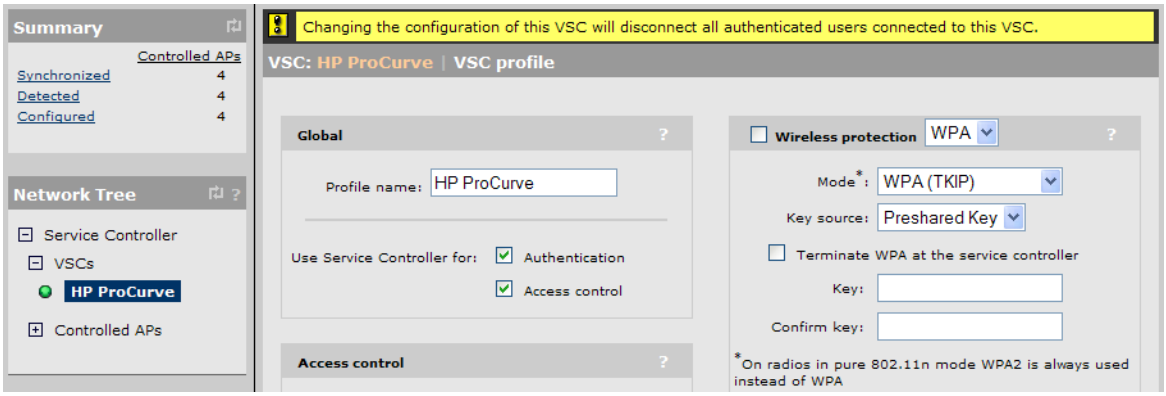
The VSC profiles list shows all VSCs are that are currently defined on the service controller. To open the list, select **VSCs** in the **Network Tree**.



The **HP ProCurve** VSC profile is predefined.

- To add a VSC, select **VSCs >> Overview > Add New VSC Profile**.
- To edit a VSC, select its name in the VSC list, or in the Network Tree.

In either case, the VSC profile page opens. In this page sample, only the top of the VSC profile page is shown.



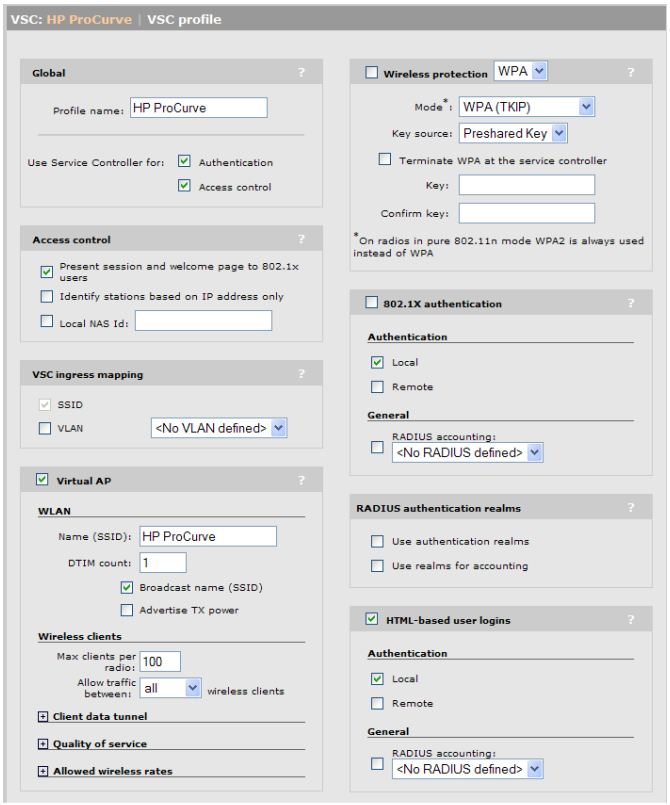
The default VSC

The default VSC is used as a fallback for any traffic that goes through the service controller and that cannot be identified as coming from an MSM AP. It is also used to handle all non-VLAN traffic from wired devices connected to the service controller's LAN port (i.e., traffic from 3rd-party APs or wired users on the network). See *About the default VSC on page 2-25*.

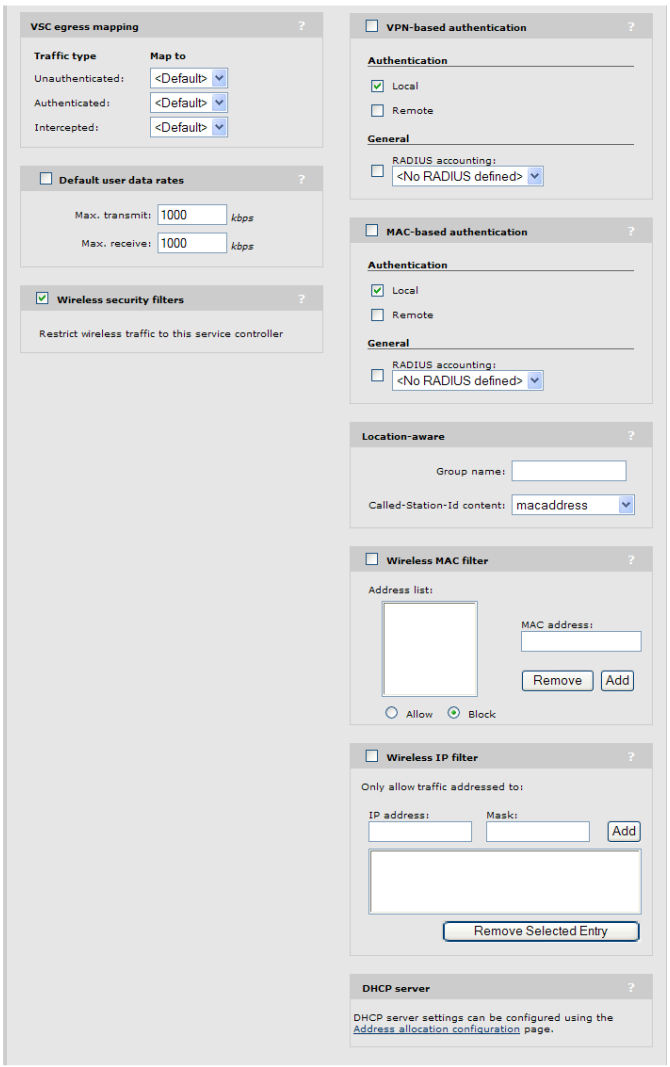
VSC configuration options

This section provides an overview of all the configuration options available for a VSC. It will give you a good idea on how the features can be used. For detailed information on each option and its settings, see the online help.

The default VSC is pre-configured as follows.

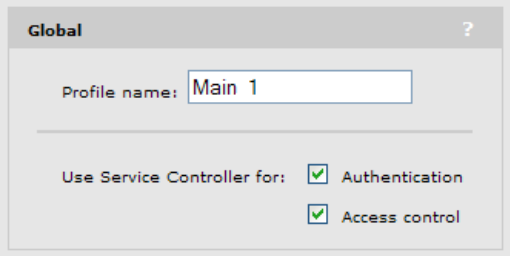


Continued from below left



About access control and authentication

The availability of certain VSC features and their functionality is controlled by the settings of two important parameters in the **Global** box. These parameters determine how authentication and access control are handled by the VSC:



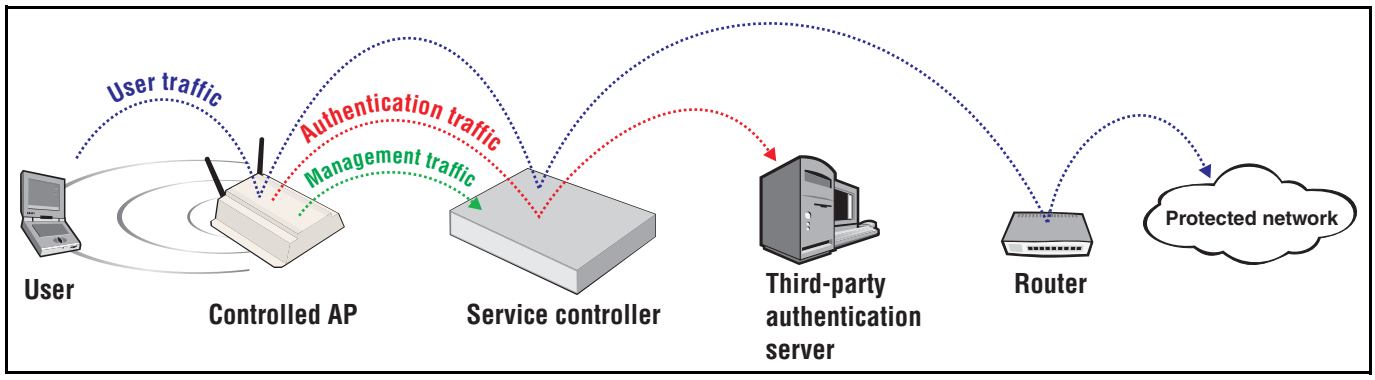
Use Service Controller for: Authentication
Determines if user authentication services (802.1X, WPA, WPA2) are provided by the service controller. When enabled, APs forward user login requests to the service controller. The service controller resolves these requests using the local user accounts, or Active Directory, or acts as a RADIUS proxy for a third-party RADIUS server.

Use service controller for: Access control
This option can only be enabled if the **Authentication** option is enabled first. When enabled, this option creates an access-controlled VSC. This means that access to protected network resources via this VSC are restricted by the access control features on the service controller. Access control features include the public access interface and access lists.

The following diagrams provide an overview of how user authentication and data traffic are handled depending on how these options are configured.

When both authentication and access control are enabled on a VSC

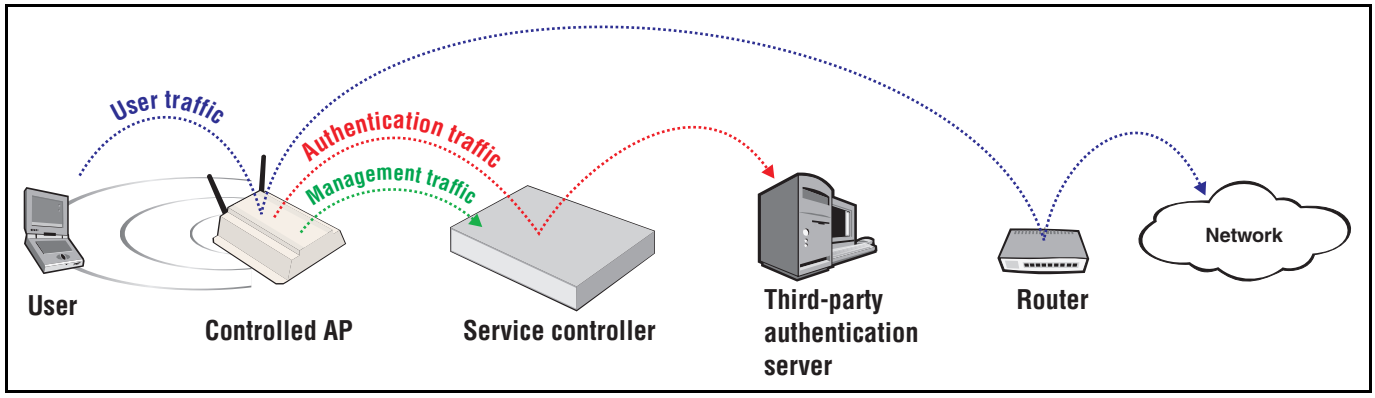
In this configuration, the controlled AP forwards authentication requests from users on the VCSC to the service controller. The service controller resolves these requests using the local user list, or the services of a third-party authentication server (Active Directory or RADIUS server). The service controller then manages access to the protected network using its access control features (public access, interface, access lists, etc).



When only authentication is enabled on a VSC

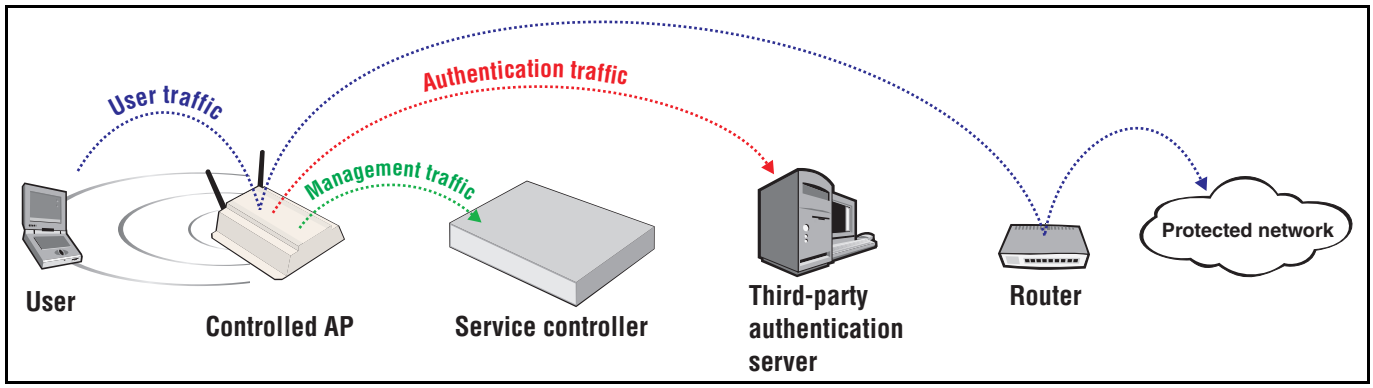
In this configuration, the controlled AP forwards authentication requests from users on the VCSC to the service controller. The service controller resolves these requests using the local user list, or the services of a third-party authentication server (Active Directory or RADIUS server).

The controlled AP forwards all authenticated user traffic from users on the VCSC to the protected network (or another device performing access control) according to settings defined on the controlled AP.



When neither option is enabled

In this configuration, the controlled AP resolves authentication requests using a third-party RADIUS server and forwards authenticated user traffic to the protected network (or another device performing access control). In this scenario, the service controller is used for management of the AP only.



Summary of VSC configuration options

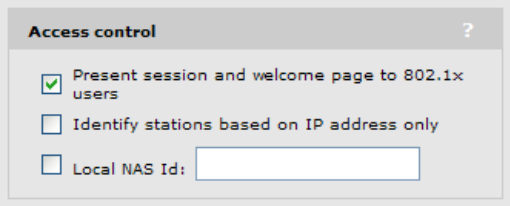
The following table lists the VSC configuration options that are available depending on how access control and authentication are configured.

VSC configuration option	Use service controller for:		
	Authentication and Access control	**Authentication only**	**Neither**
Access control	■		
Virtual AP	■	■	■
VSC ingress mapping	■		
VSC egress mapping	■		
Default user data rates	■		
Wireless mobility		■	■
Wireless security filters	■	■	■
Wireless protection	■	■	■
802.1X authentication	■	■	■
RADIUS authentication realms	■	■	
HTML-based user logins	■		
VPN-based authentication	■		
MAC-based authentication	■	■	■
Location-aware	■		
Wireless MAC filter	■	■	■
Wireless IP filter	■	■	■
DHCP server	■		
DHCP relay	■		

The sections that follow provide an overview and use of each VSC option. For complete descriptions of individual parameters see the online help in the management tool.

Access control

Enabling the **Present session and welcome page to 802.1X users** means that 802.1X users will see the public access interface Session page after they log in.

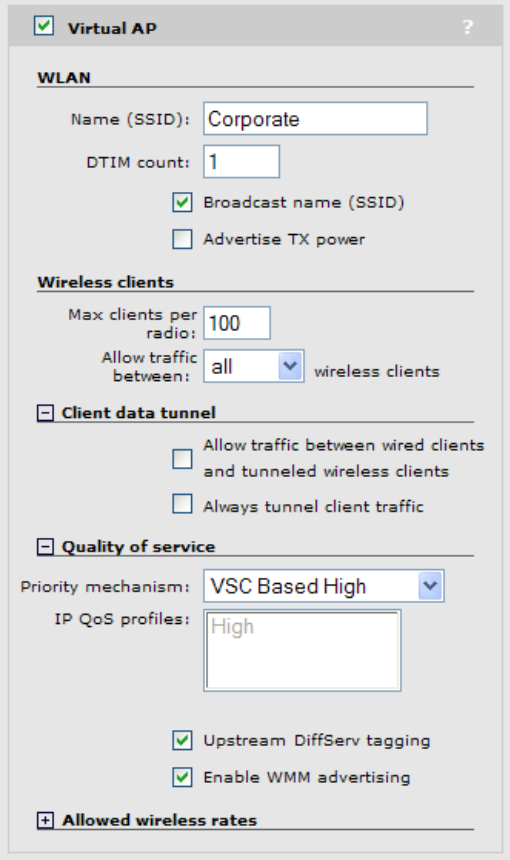


Note

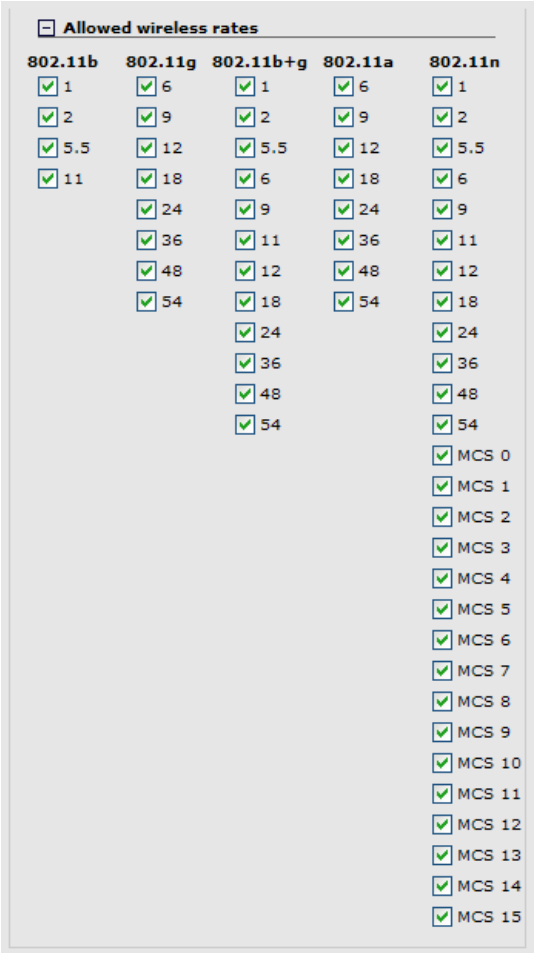
Display of the Session page may not work for all users. It will fail if the initial traffic from the user's computer is sent by an application other than the user's browser. For example: messaging software, automatic software update services, email applications.

Virtual AP

These settings define the characteristics of the wireless network created by the VSC, including its name, the number of clients supported, and QoS settings.



Continued from below left



Client data tunnel

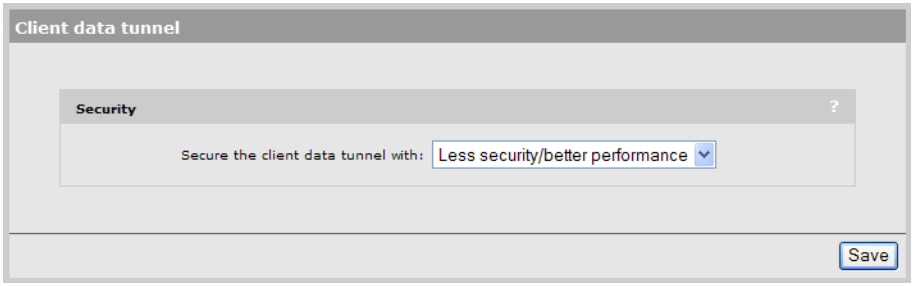
When a VSC is access-controlled, client traffic that is sent between the AP and service controller can be carried in the client data tunnel. This provides the following benefits:

- User traffic is segregated from the backbone network and can only travel to the service controller.
- Underlying network topology is abstracted enabling full support for L2-connected users across routed networks.

The client data tunnel is always used when the connection between a controlled AP and its service controller traverses at least one router. The client data tunnel supports NAT traversal, so it can cross routers that implement NAT.

Optionally the client data tunnel can also be used when a controlled AP and its service controller are on the same subnet. To do this, enable the **Always tunnel client traffic** option.

Performance and security settings for the client data tunnel can be customized on the **Service controller >> Controlled APs > Client data tunnel** page.



- **Less security/better performance**: The default provides adequate security with better performance.
- **High security/less performance**: Provides maximum security but with reduced performance.

The client tunnel does not encrypt the data stream. To protect client traffic with encryption requires that client stations use WPA or VPN software.

- Under **Wireless protection**, enable **WPA** with the **Terminate WPA at the service controller.** This requires client stations that support WPA.
- Use **VPN-based authentication**. See *Securing wireless client sessions with VPNs on page 12-3*.

Quality of service

Lets you prioritize traffic on the VSC. See *Quality of service (QoS) on page 2-25*.

Allowed wireless rates

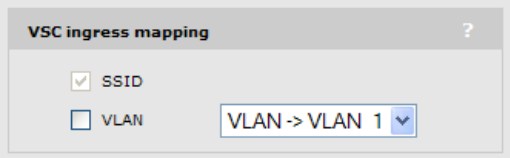
Lets you select the wireless transmission speeds that are supported for each wireless mode.

MSM410 and MSM422 only: For 802.11n, in addition to speeds 1 to 54, 16 MCS values (MCS0 to MCS15) are also included, with MCS0 being the slowest and MCS15 being the fastest.

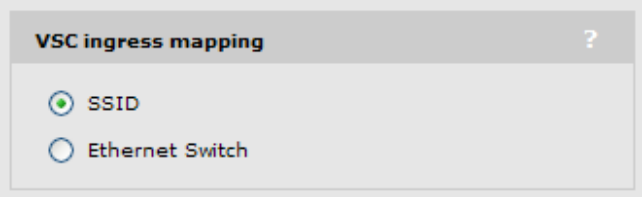
VSC ingress mapping

These settings apply to the service controller only and define how ingress traffic on the LAN port is assigned to a VSC. See *VSC data flow on page 2-21*.

When access control is enabled, available options are:



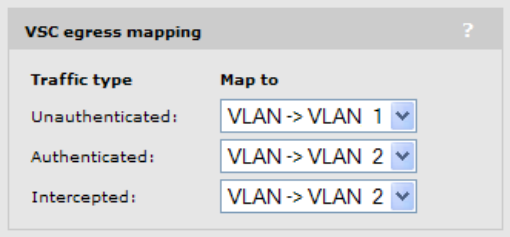
When access control is disabled, available options are:



The Ethernet Switch option enables the VSC to be bound to specific ports on an MSM317. See the *MSM317 Access Device Installation and Getting Started Guide*.

VSC egress mapping

These options select the service controller output interface on which a VSC forwards user traffic. (To set VSC egress options for controlled APs, see *Binding a VSC to a group on page 3-24*.) Different types of traffic can be forwarded to different output interfaces, which include the routing table, VLAN ID, or an IP GRE tunnel. Before you can map traffic to an output interface, the interface must already be defined. See *VSC data flow on page 2-21*.



In the above example, with all defaults selected, the service controller routing table is used for all egress traffic. Therefore, all ingress traffic on this VSC is routed according to the routes defined on the **Service Controller >> Network > IP routes** page.

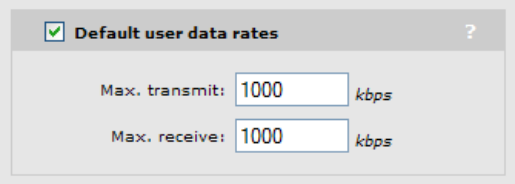
Note

Traffic from specific users can be **Intercepted**. To enable traffic interception for a specific user, you must specify the appropriate setting in the user's RADIUS account. See *Colubris-Intercept on page 9-22*.

Default user data rates

These options enable you to set the default data rates for authenticated users that do not have a data rate set in their RADIUS accounts and unauthenticated users. For details on setting the appropriate RADIUS attributes to accomplish this, see *Chapter 8: Public/guest network access* and *Chapter 9: Working with public access attributes*.

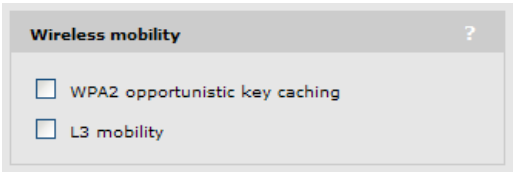
The throughput limits globally defined on the **Service Controller >> Network > Bandwidth control** page always take precedence over user data rates. This means if you set a data rate which exceeds the configured bandwidth level, the rate will be capped at the bandwidth level.



Wireless mobility

Mobility services are only available when **Access control** is disabled (under **General**) and the Mobility license is installed. See *Mobility license on page 11-2*.

- WPA2 opportunistic key caching eliminates the delays associated with reauthentication when users roam between APs on the same layer 2 network. This also requires that WPA2 be used.
- Layer 3 mobility enables users to move between APs that are connected to different IP subnets while maintaining their assigned IP address. Typical applications are VoWLAN and the roaming and maintaining of VoWLAN calls when moving between subnets.

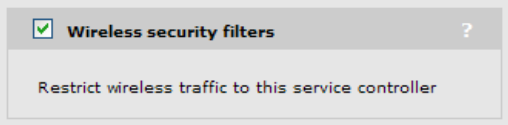


See *Chapter 11: Wireless mobility*.

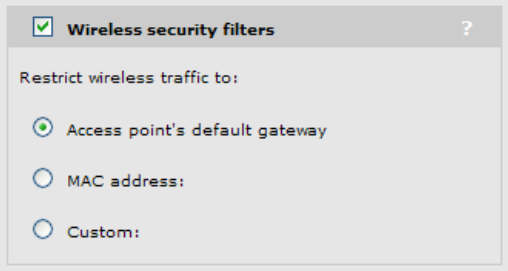
Wireless security filters

APs feature an intelligent bridge that can apply security filters to safeguard the flow of wireless traffic. These filters limit both incoming and outgoing traffic as defined below and force the APs to exchange traffic with a specific upstream device.

- If **Access control** is enabled (under **General**), the controlled AP will only allow user traffic that is addressed to the service controller. All other traffic is blocked. Make sure that the service controller is set as the default gateway for all users. If not, all user traffic will be blocked by the AP.



- If **Access control** is disabled (under **General**), then the security filters can be used to block traffic unless it is addressed to a specific device.



  Use the **Custom** option to define a custom filter with standard pcap syntax and a few HP ProCurve Networking-specific placeholders. See the online help for details.

Wireless protection

Two types of wireless protection are offered. WPA and WEP.

- **MSM410 and MSM422 only:** When using 802.11n, WEP protection is never permitted. If selected, WPA or WPA2 protection is used instead. Also, when using pure 802.11n in either the 2.4 or 5 GHz bands, WPA2 protection is used regardless of wireless protection setting that is chosen.

WPA

This option enables support for users with WPA / WPA2 client software.

Mode
Support is provided for

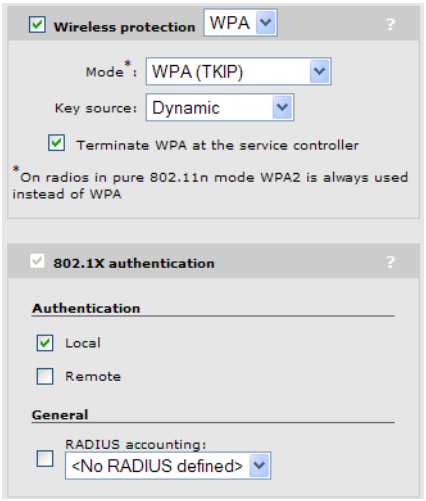
- **WPA (TKIP)**: WPA with TKIP encryption.
- **WPA2 (AES/CCMP)**: WPA2 (802.11i) with AES/CCMP encryption.
- **WPA or WPA2**: Mixed mode supports both WPA (version 1) and WPA2 (version 2) at the same time.

Key source

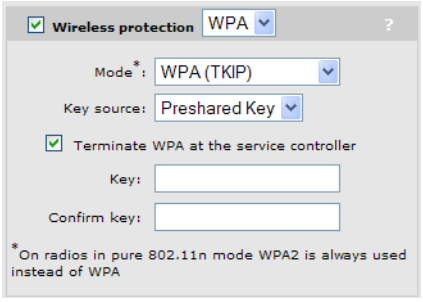
This option determines how the TKIP keys are generated.

- **Dynamic**: This is a dynamic key that changes each time the user logs in and is authenticated. The MPPE key is used to generate the TKIP keys that encrypt the wireless data stream. The key is generated via the configured **802.1X authentication** method. Therefore, when you enable this option, the **802.1X authentication** feature is automatically enabled.

  Authentication can occur via the local user accounts and remote authentication server (Active Directory, or third-party RADIUS server). If both options are enabled, the local accounts are checked first.



- **Preshared Key**: The service controller uses the key you specify in the **Key** field to generate the TKIP keys that encrypt the wireless data stream. Since this is a static key, it is not as secure as the RADIUS option. Specify a key that is between 8 and 63 alphanumeric characters in length. It is recommended that the preshared key be at least 20 characters long, and be a mix of letters and numbers. The double quote character (") should not be used.



Terminate WPA at the service controller

Note This feature is intended for low-data-volume applications like that of wireless POS terminals.

This option controls the termination of WPA/WPA2 client sessions.

- When enabled, the service controller acts as the termination point for all WPA/WPA2 sessions.
- When disabled, WPA/WPA2 sessions are terminated at the AP.

To use this option, the client device must be WPA capable.

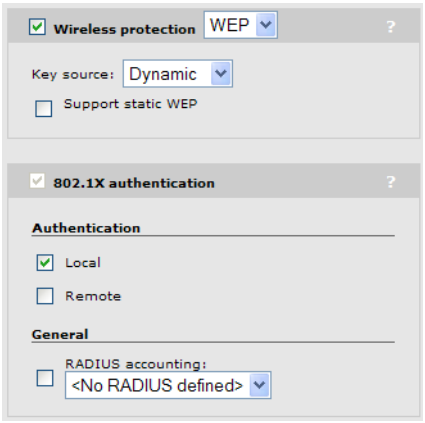
Normally (with **Terminate WPA at the service controller** disabled) only the wireless portion of the communication (between the user and AP) is secured, and the AP to service controller portion is not. This is normally sufficient since outsiders have no access to your wired network. However, in a public venue such as a hotel, if the public has access to your wired network, it may be necessary
to secure communications all the way from the wireless client to the service controller.

WEP

This option provides support for users using WEP encryption.

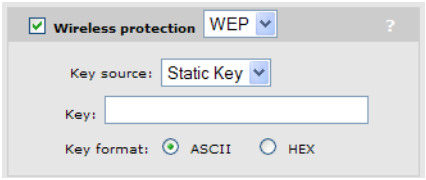
Key source
This option determines how the WEP keys are generated: Dynamic or Static Key.

- **Dynamic**: This is a dynamic key that changes each time the user logs in and is authenticated. The key is generated via the configured **802.1X authentication** method. Therefore, when you enable this option, the **802.1X authentication** feature is automatically enabled.



Support static WEP: Enables support for users that are using the specified static WEP key. See the definitions below for information on how to define the key.

- **Static key**: This is a static key that you must define.



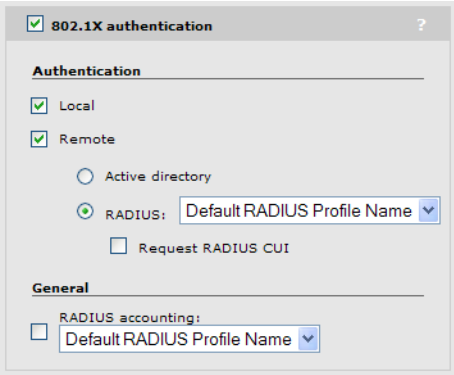
  - **Key:** The number of characters you specify for the key determines the level of encryption. For 40-bit encryption, specify 5 ASCII characters or 10 HEX digits. For 128-bit encryption, specify 13 ASCII characters or 26 HEX digits.

When encryption is enabled, wireless stations that do not support encryption cannot communicate with the AP. The definition for each encryption key must be the same on the AP and all client stations.

- **Key format:** Select the format used to specify the encryption key:
  - **ASCII:** ASCII keys are much weaker than carefully chosen HEX keys. You can include ASCII characters between 32 and 126, inclusive, in the key. However, note that not all client stations support non-alphanumeric characters such as spaces, punctuation, or special symbols in the key.
  - **HEX:** Your keys should only include the following characters: 0-9, a-f, A-F

802.1X

This option enables support for users with 802.1X client software that use any of the following authentication methods: EAP-TLS, EAP-TTLS, and EAP-PEAP. Additionally, when an external RADIUS server is used, support for EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC is also provided. Check your external RADIUS server for supported authentication methods.

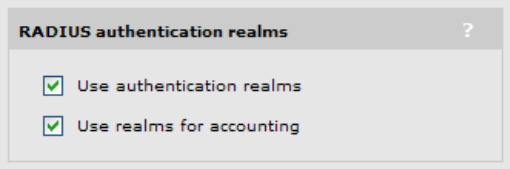


Note If 802.1X is used without enabling WEP, wireless traffic will be unencrypted.

RADIUS authentication realms

When realms are enabled for accounting or authentication, selection of the RADIUS server to use is based on the realm name. If no match is found, then the configured RADIUS profile name is used.

This applies to any VSC authentication or accounting setting that uses a RADIUS server.



Note

The VSC-defined RADIUS server becomes the default when no servers based on the realm are detected.

Realm names are extracted from user names as follows: if the username is **person1@mydomain.com** then **mydomain.com** is the realm. The authentication request is sent to the RADIUS profile with the realm name **mydomain.com**. The username sent for authentication is still the complete **person1@mydomain.com**.

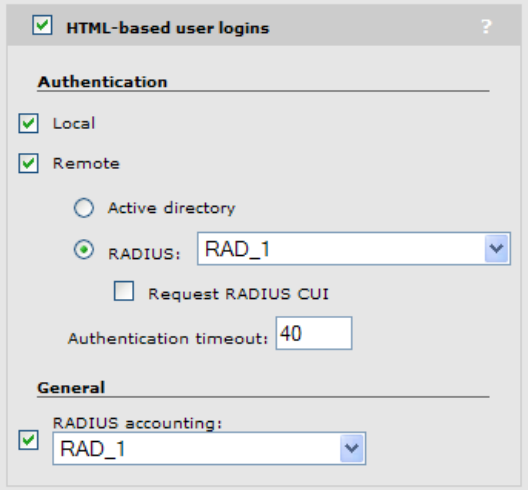
For added flexibility, regular expressions can be used in realm names, enabling a single realm name to match many users. For example, if a realm name is defined with the regular expression **^per.*** then all usernames beginning with **per** followed by any number of characters will match. The following usernames would all match:

per123.biz
per321.lan
per1

HTML-based user logins

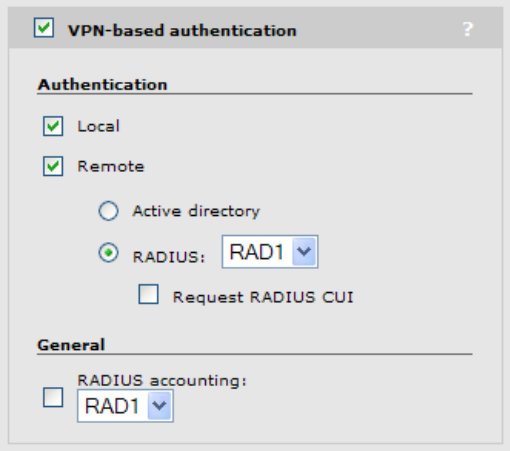
This option defines settings for users who log in to the public access interface using a Web browser. If you disable this option, the public access interface Login page is not shown to these users. However, login is still possible via other methods such as MAC authentication and 802.1X.

Authentication can occur via the local user accounts and a remote server (Active Directory or RADIUS). If both options are enabled, the local user accounts are always checked first.



VPN-based authentication

This option defines settings for users who log in to the public access interface using a VPN connection. To use this option a VPN must be configured for securing wireless client sessions. See *Securing wireless client sessions with VPNs on page 12-3*.



See the online help for details.

Notes for PPTP server

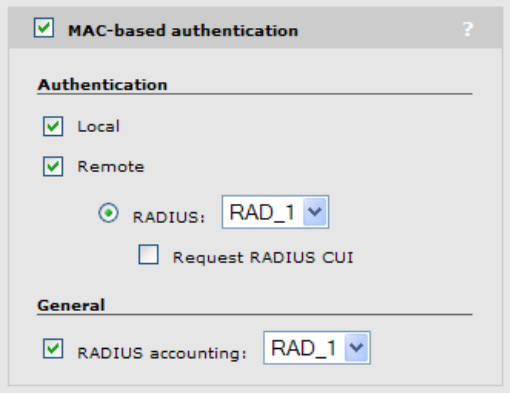
- If you enable this option for a VSC, all wireless users on the VSC must establish a PPTP connection. All other authentication methods (HTML, MAC) cannot be used.
- If you enable this option on the default VSC, all wired users must establish a PPTP connection. (Wired users always connect to the default VSC.)
- When configuring user PPTP software, the address of the PPTP server is the one assigned to the service controller LAN port.

MAC-based authentication

Note

This option can only be used to authenticate wireless users. If used on the first VSC or any other VSC that supports both wired and wireless users, wired users gain access without having to authenticate.

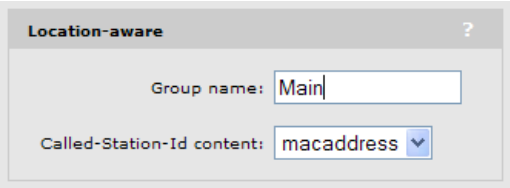
This option enables wireless users to be authenticated by their MAC addresses. Authentication can occur via the local user accounts and a remote RADIUS server. If both options are enabled, the local user accounts are checked first.



Location-aware

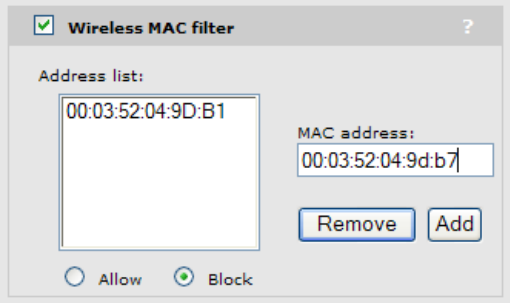
This option enables you to control logins to the public access network based on the AP, or group of APs, to which a user is connected. It is automatically enabled when a VSC is set to **Access control**. Location-aware is always enabled when using the service controller for authentication or access-control with a remote RADIUS server.

For each user login, location-aware sends the PHY Type, SSID, and VLAN to the remote RADIUS server. It also includes the specified **Called-Station-Id content**.



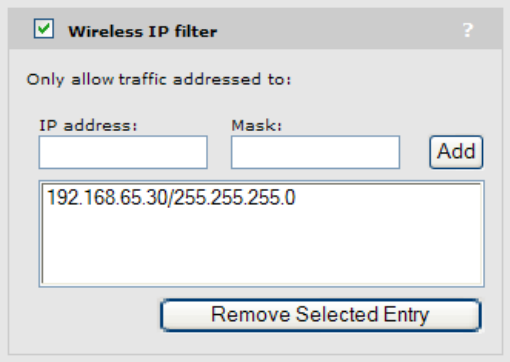
Wireless MAC filter

This option enables you to control access to the wireless network based on the MAC address of device. You can either block access or allow access, depending on your requirements.



Wireless IP filter

This option enables you to allow only wireless-to-wired LAN traffic for specific destination addresses.



DHCP server

This option is only available if the service controller is configured as a DHCP server on the **Service Controller >> Network > Address allocation** page. See *Address allocation on page 10-6*.

A separate DHCP server can be enabled on each VSC to provide custom addressing to users. This enables you to assign different IP address ranges for each VSC. To receive traffic from users, the service controller assigns the **Gateway** address you specify to its LAN port.

Note

These configuration options do not appear for the default VSC. The default VSC uses the same settings as defined on the **Service Controller >> Network > Address allocation** page.

DHCP relay agent

This option is only available if the service controller is currently configured as a DHCP relay agent on the **Service Controller >> Network > Address allocation** page. See *Address allocation on page 10-6*.

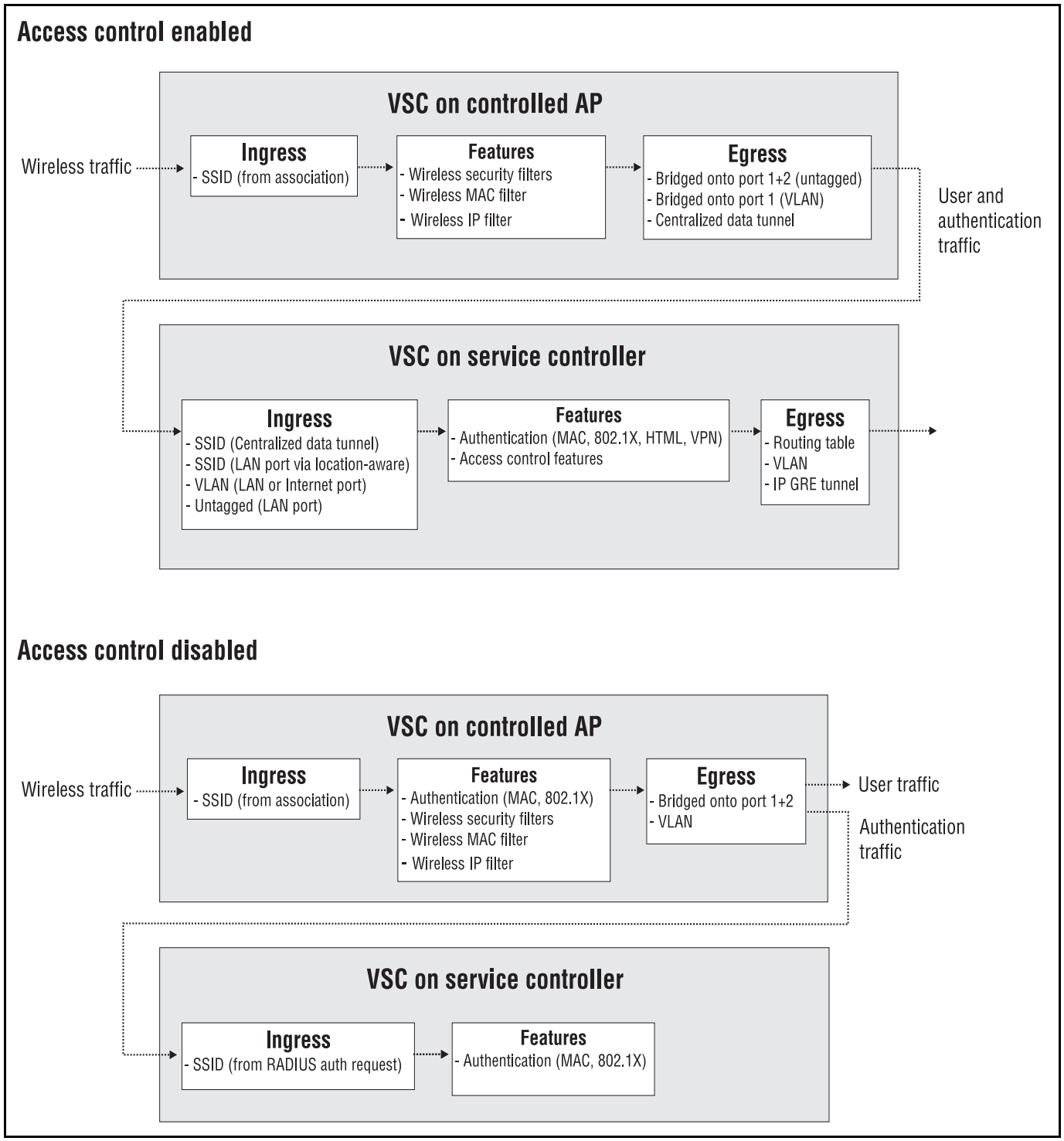
A separate DHCP relay agent can be enabled on each VSC to provide custom addressing to users.

Note

These DHCP relay agent options do not appear for the default VSC. The default VSC uses the same settings as defined on the **Service Controller >> Network > Address allocation** page.

VSC data flow

Each VSC provides a number of configurable options, some of which apply exclusively on controlled APs or the service controller. The following diagrams illustrate how traffic from **wireless users** is handled by VSC definitions on a **controlled AP** and service controller, and shows the options that apply on each device.



Access control enabled

VSC on controlled AP

Ingress

The AP only handles wireless traffic. The SSID is the name of the wireless network with which the user associates.

Features

- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific destination, such as the service controller. See *Wireless security filters on page 2-13*.
- **Wireless MAC filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.
- **Wireless IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses.

Egress

- **Bridged onto port 1+2 (untagged):** Untagged user and authentication traffic is bridged onto ports 1 and 2.
- **Bridged onto port 1 (VLAN):** VLAN tagged traffic is bridged onto port 1 only. VLAN tags can be assigned on a per-user basis via RADIUS attributes (see *Defining account profiles on page 7-11*), or for all traffic on a VSC (see *Defining VLANs on page 3-28*).
- **Client data tunnel:** When this option is enabled, the AP creates a data tunnel to the service controller to carry all user traffic. See *Client data tunnel on page 2-10*.

VSC on service controller

Ingress

- **SSID (Client data tunnel):** When a client data tunnel has been created between the AP and the service controller, all user traffic comes in on it. See *Client data tunnel on page 2-10*. The tunnel is established using same interface on which the AP was discovered. (LAN or Internet port).
- **SSID (LAN port):** SSID is retrieved using the location-aware function.
- **VLAN (LAN or Internet port):** Traffic with a VLAN ID is handled by the VSC with a matching VLAN definition. See *Using multiple VSCs on page 2-24*.
- **Untagged (LAN port):** Untagged traffic on the LAN port may originate from wired users, or MSM APs operating in autonomous mode.

Features

- **Authentication:** The service controller supports 802.1X, MAC, or HTML authentication. To validate user login credentials the service controller can use the local user accounts or make use of a third-party authentication server (Active Directory or RADIUS). See *Authentication types on page 7-3*.
- **Access control features:** The service controller provides a number of features that can be applied to user sessions. Features can be enabled globally or on a per-account basis. See *Account profiles on page 7-6*.

Egress

The service controller enables user traffic to be forwarded to different output interfaces, which include the routing table, VLAN ID, or GRE tunnel. See *VSC egress mapping on page 2-11*.

Access control disabled

VSC on controlled AP

Ingress

The AP only handles wireless traffic. The SSID is the name of the wireless network that the user associates with.

Features

- **Authentication:** The AP supports 802.1X or MAC authentication. To validate user login credentials the AP makes use of a third-party authentication server (service controller or third-party RADIUS server). See *Authentication types on page 7-3*.
- **Wireless security filters:** Enables the AP to block traffic unless it is addressed to a specific destination (like the service controller). See *Wireless security filters on page 2-13*.
- **Wireless MAC filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user MAC addresses.
- **Wireless IP filter:** Enables the AP to only allow wireless-to-wired LAN traffic for specific wireless-user IP addresses.

Egress

- **Bridged onto port 1+2:** Unless a centralized mode tunnel has been established, user and authentication traffic is bridged onto ports 1 and 2.
- **VLAN:** VLAN tags can be assigned for all traffic on a VSC. See *Defining VLANs on page 3-28*.

VSC on service controller

Ingress

- **SSID (from RADIUS auth request):** The service controller determines the SSID from the RADIUS authentication request sent by the AP, and uses this SSID to determine the VSC to use for authentication.

Features

- **Authentication:** The service controller supports 802.1X or MAC authentication. To validate user login credentials the service controller can use the local user accounts or make use of a third-party authentication server (Active Directory or RADIUS). See *Authentication types on page 7-3*.

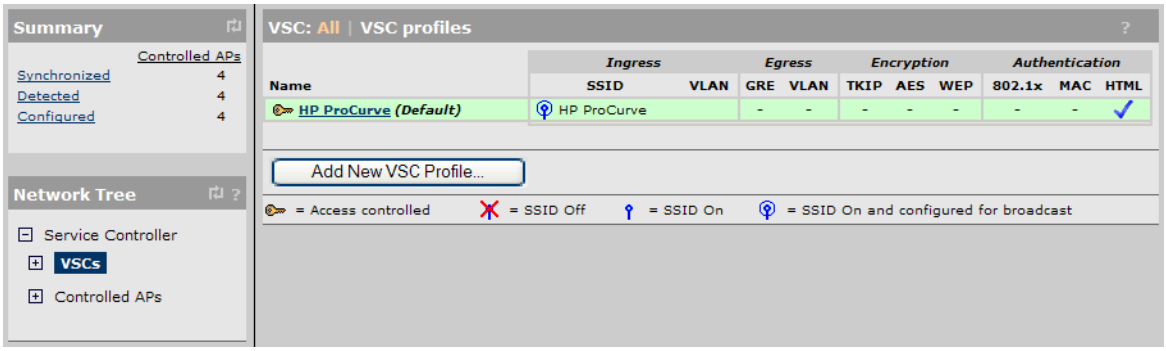
Using multiple VSCs

When multiple VSCs are defined, it is important to know how user traffic is matched to a VSC definition. When VSCs have access control enabled, incoming traffic is handled on the service controller as follows:

Incoming traffic properties	Port	If ...	Then ...
SSID and untagged	LAN	VSC with matching SSID exists	Traffic is sent on the egress mapping defined on the matching VSC.
		No VSC with matching SSID exists	Traffic is sent on the egress mapping defined on the default VSC.
SSID and VLAN or VLAN only	LAN or Internet	VSC with matching Ingress VLAN exists.	Traffic is sent on the egress mapping defined on the matching VSC.
		VLAN exists in VLAN table (but is not assigned to a VSC ingress.	Traffic is routed according to the global routing table.
		No VLAN exists.	Traffic is blocked.
Untagged	LAN		Traffic is sent on the egress mapping defined on the default VSC.

About the default VSC

The default VSC is automatically created by the service controller. It is identified with the label **(default)** in the VSC list. Initially, this VSC is named **HP ProCurve**.



Traffic from wired users is always handled by the default VSC as follows:

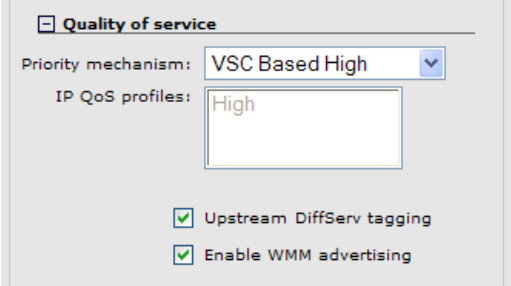
- **When access control is disabled on the default VSC**, traffic from wired users connected to the service controller LAN port is blocked.
- **When access control is enabled on the default VSC**, traffic from authenticated wired users connected to the service controller LAN port is sent on the egress mapping defined on the default VSC. If HTML and 802.1X based authentication methods are disabled, traffic from all users is sent on the egress mapping without the need for authentication.

Note

If only MAC-based authentication is defined on the default VSC, wired users gain access to the network without being authenticated. Wireless users however, must log in because MAC-based authentication applies to wireless users only.

Quality of service (QoS)

The quality of service (QoS) feature provides a number of different mechanisms to prioritize wireless traffic sent to wireless client stations. This is useful when the service controller handles wireless traffic from multiple devices (or multiple applications on a single device), that have different data flow requirements.



The QoS feature defines four traffic queues based on the Wi-Fi Multimedia (WMM) access categories. In order of priority, these queues are:

Queue	WMM access category	Typically used for
1	AC_VO	Voice traffic
2	AC_VI	Video traffic
3	AC_BE	Best effort data traffic
4	AC_BK	Background data traffic

Outgoing wireless traffic on the VSC is assigned to a queue based on the selected priority mechanism. Traffic delivery is based on strict priority (per the WMM standard). Therefore, if excessive traffic is present on queues 1 or 2, it will reduce the flow of traffic on queue 3 and queue 4.

Regardless of the priority mechanism that is selected:

- Traffic that cannot be classified by a priority mechanism is assigned to queue 3.
- SVP (SpectraLink Voice Protocol) traffic is always assigned to queue 1, except if you select the VSC-based priority mechanism, in which case SVP traffic is assigned to the configured queue.

Priority mechanisms

Priority mechanisms are used to classify traffic on the VSC and assign it to the appropriate queue. The following mechanisms are available:

802.1p

This mechanism classifies traffic based on the value of the VLAN priority field present within the VLAN header.

Queue	802.1p (VLAN priority field value)
1	6,7
2	4,5
3	0,2
4	1,3

VSC-based priority

This mechanism is unique to HP ProCurve Networking. It enables you to assign a single priority level to all traffic on a VSC. If you enable the VSC-based priority mechanism, it takes precedence regardless of the priority mechanism supported by associated client stations. For example, if you set VSC-based low priority, then all devices that connect to the VSC have their traffic set at this priority, including SVP clients.

Queue	VSC-based priority value
1	Very-based Very High
2	Very-based High
3	Very-based Normal
4	Very-based Low

DiffServ (Differentiated Services)

This mechanism classifies traffic based on the value of the Differentiated Services (DS) codepoint field in IPv4 and IPv6 packet headers (as defined in RFC2474). The codepoint is composed of the six most significant bits of the DS field.

Queue	DiffServ (DS codepoint value)
1	111000 (Network control) 110000 (Internetwork control)
2	101000 (Critical) 100000 (Flash override)
3	011000 (Flash) 000100 (Routine)
4	010000 (Immediate) 001000 (Priority)

TOS

This mechanism classifies traffic based on value of the TOS (Type of Service) field in an IP packet header.

Queue	TOS (Type of Service field value)
1	0x30, 0xE0, 0x88, 0xB8
2	0x28, 0xA0
3	0x08, 0x20
4	All other TOS traffic

IP QoS

This option lets you assign traffic to the queues based on the criteria in one or more IP QoS profiles. Each profile lets you target traffic on specific ports or using specific protocols.

Disabled

When QoS traffic prioritization is disabled, all traffic is sent to queue 3.

IP QoS profiles

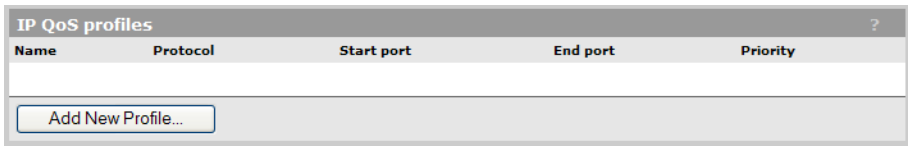
This option is only available if you set the **Priority mechanism** to **IP QoS**.

Select the IP QoS profiles to use for this profile. To add QoS profiles to the list, use the **Network > IP QoS** page.

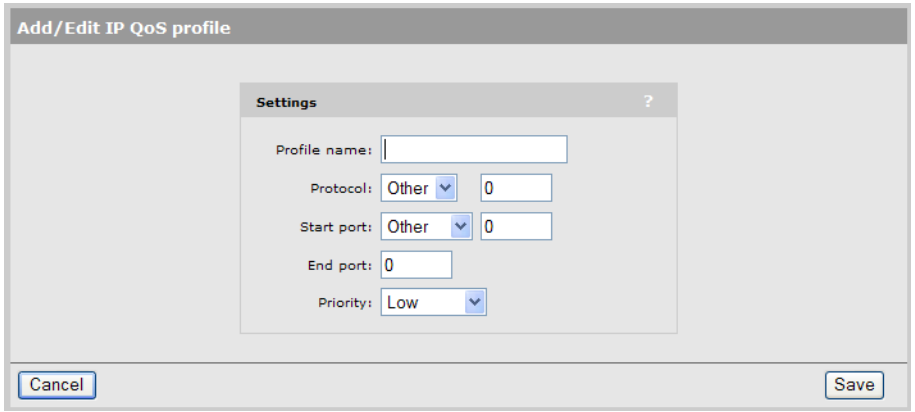
Up to 10 profiles can be selected. To select more than one profile, hold down the CTRL key as you select profile names in the list.

To define an IP QoS profile

1. Select **Service Controller >> Network > IP QoS**. Initially, no profiles are defined.



2. Select **Add New Profile**.



3. Configure parameter settings as follows:

Settings

Profile name
Specify a unique name to identify the profile.

Protocol
Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually. You can find IANA-assigned protocol numbers on the Internet.

Start port/ End port
Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both **Start port** and **End port.** Port numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually.

Note To accept traffic on all ports for a specified protocol, set **Start port** to **Other** and **0.**

Priority
Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.

Note It is strongly recommended that you reserve **Very high** priority for voice applications.

Upstream DiffServ tagging

Enable this option to have the M111 apply differentiated services marking to upstream traffic.

Layer 3 upstream marking ensures end-to-end quality of service in your network. Data originating on the wireless network can now be carried throughout the network (wireless *and* wired) with a consistent quality of service and priority. This feature is enabled by default.

When this feature is enabled, packets received on the wireless interface that include Wi-Fi Multimedia (WMM) QoS values are remarked using IP TOS/DiffServ values when transmitted to the wired network.

Upstream/downstream traffic marking

Depending on the priority mechanism that is active, upstream and downstream traffic is marked as described in this section.

Upstream traffic marking

This table describes the marking applied to wireless traffic sent by connected client stations to the service controller and then forwarded onto the wired network by the service controller.

Mechanism	**INCOMING TRAFFIC** Wireless traffic sent from client stations to the AP	**OUTGOING TRAFFIC** Traffic sent by the AP to the network		
		L2 marking	**L3 marking**	
			Upstream DiffServ tagging is enabled	**Upstream DiffServ tagging is disabled**
802.1p	WMM	802.1p (requires an egress VLAN to be defined for the VSC)	DiffServ	Pass-through (Original layer 3 marking, if any, is preserved.)
DiffServ	DiffServ			
TOS	TOS			
VSC-based	WMM Non-WMM	802.1p (requires an egress VLAN to be defined for the VSC)		
IP QoS	WMM			

Downstream traffic marking

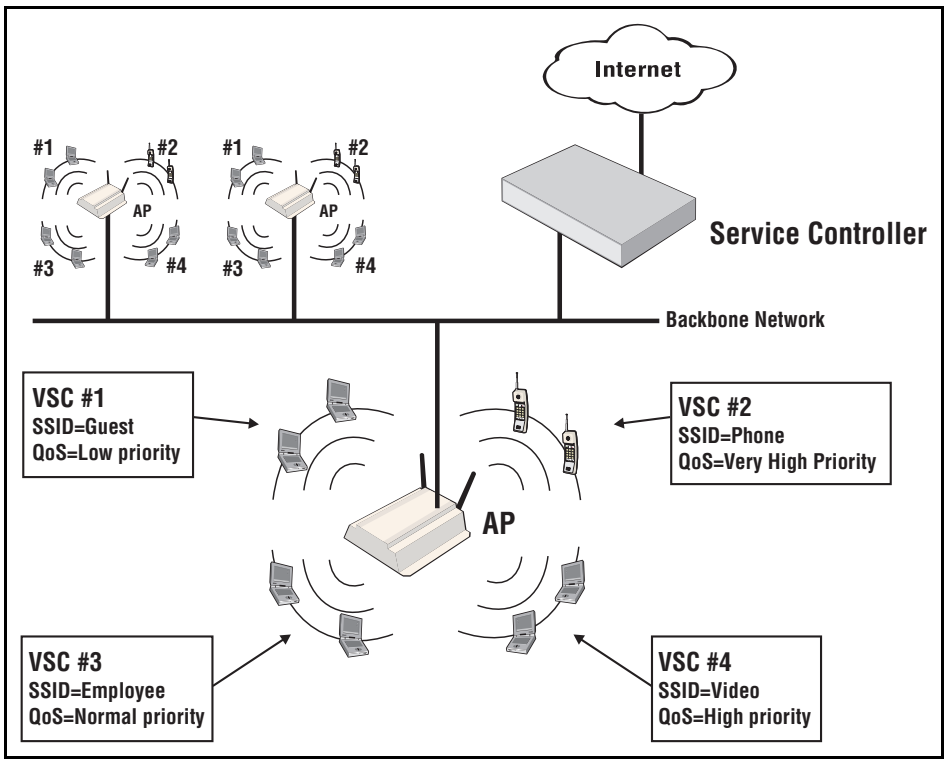
This table describes the marking applied to traffic received from the wired network by the service controller and then sent to connected wireless client stations.

Mechanism	**INCOMING TRAFFIC** Traffic received from wired network	**OUTGOING TRAFFIC** Wireless traffic sent from the service controller to client stations	
		WMM Client	**Non-WMM Client**
802.1p	802.1p	WMM + HPQ (WMM marking done according to the rules for the mechanism.)	HPQ (hardware priority queueing)
DiffServ	DiffServ		
TOS	TOS		
VSC-based	All traffic on the VSC		
IP QoS	All traffic that matches the ports/protocols specified in the selected IP QoS profiles		

Note Although the WMM specification refers to 802.1D and not 802.1p, this guide uses the term 802.1p because it is more widely recognized. (The updated IEEE 802.1D: ISO/IEC 15802-3 (MAC Bridges) standard covers all parts of the Traffic Class Expediting and Dynamic Multicast Filtering described in the IEEE 802.1p standard.)

QoS example

In this QoS example a single service controller provides voice and data wireless support with different quality of service settings for guests and employees.



VSCs are defined with the following SSIDs and QoS settings:

- **Phone**: Supports wireless phones using very high priority.
- **Video**: Supports high-priority video traffic for video conferences.
- **Employee**: Used by employees. Features a higher QoS setting than the guest profile.
- **Guest**: Used by guests. Guest get the lowest traffic priority, to reserve bandwidth for employees.

Creating a new VSC

To add a VSC, select **Service Controller > VSCs >>VSC Profiles > Add New VSC Profile**.

Define VSC parameters and select **Save**. Familiarize yourself with sections of interest in *VSC configuration options on page 2-5*. See the online help for parameter descriptions.

Assigning a VSC to a group

When working with controlled APs, VSC definitions must be bound to a group so that they will automatically be activated on the APs in the group. For information on how to bind (assign) a VSC to a group, see *Binding a VSC to a group on page 3-24*.

On the MSM317, VSCs can also be bound to a switch port. See the *MSM317 Access Device Installation and Getting Started Guide*.

Note

When working with autonomous APs, the VSC definition you create on the service controller must be manually configured on each autonomous AP. See *Working with autonomous APs on page 14-1* and the *MSM3xx/MSM4xx Management and Configuration Guide*.

3

Working with controlled APs

Contents

Key concepts 3-3

Key controlled-mode events 3-5

Discovery of controlled APs 3-7
- Discovery overview 3-7
- Discovery methods 3-8
- Discovery recommendations 3-9
- Discovery priority 3-10
- Discovery behavior 3-11
- Discovery considerations 3-12
- Monitoring the discovery process 3-13

Authentication of controlled APs 3-18
- Building the AP authentication list 3-18

Configuring APs 3-21
- Overview 3-21
- Configuration strategy 3-23
- Working with groups 3-23
- Working with APs 3-25

Defining VLANs 3-28

Provisioning 3-31
- Provisioning methods 3-31
- Displaying the provisioning pages 3-32
- Provisioning connectivity 3-34
- Provisioning discovery 3-36
- Provisioning summary 3-37

AeroScout RTLS 3-38
Software retrieval/update 3-39
Monitoring 3-39

Key concepts

The service controller provides centralized management of APs operating in controlled mode. Controlled mode greatly simplifies the set up and maintenance of a Wi-Fi infrastructure by centralizing the configuration and management of distributed APs.

Note

Starting with software version 5.x, APs operate in controlled mode by default. If you update an AP from an earlier release, the AP boots in autonomous mode. Subsequently resetting the AP to factory defaults switches it to controlled mode. For details on working with autonomous APs, see *Working with autonomous APs on page 14-1*, and *Resetting to factory defaults on page C-1*.

Plug and play installation

In most cases, initial configuration of an AP is not required. Simply power it up and plug it into a network that provides access to a service controller. The AP will automatically discover and authenticate itself with the service controller. The AP does not offer wireless services until it successfully connects with a service controller. Layer 3 networks may require the APs first to be provisioned.

Automatic software updates

Once an AP establishes a management tunnel with a service controller its software is automatically updated to match the version installed on the service controller.

Centralized configuration management

All AP configuration settings are defined using the service controller management tool and are automatically uploaded to all controlled APs with a single mouse click. For added flexibility, APs can be assigned to groups, enabling each group to have customized configuration settings. If needed, the individual settings for each AP in a group can also be customized.

Manual provisioning

By default, APs operating in controlled mode will automatically discover and connect with a service controller on most network topologies. However, in certain cases it may be necessary to manually configure (provision) connectivity and discovery options. Manual provisioning can be done directly on the AP, or via the service controller. When using the service controller, provisioning can be applied to entire groups making it easy to customize many APs at once.

Secure management tunnel

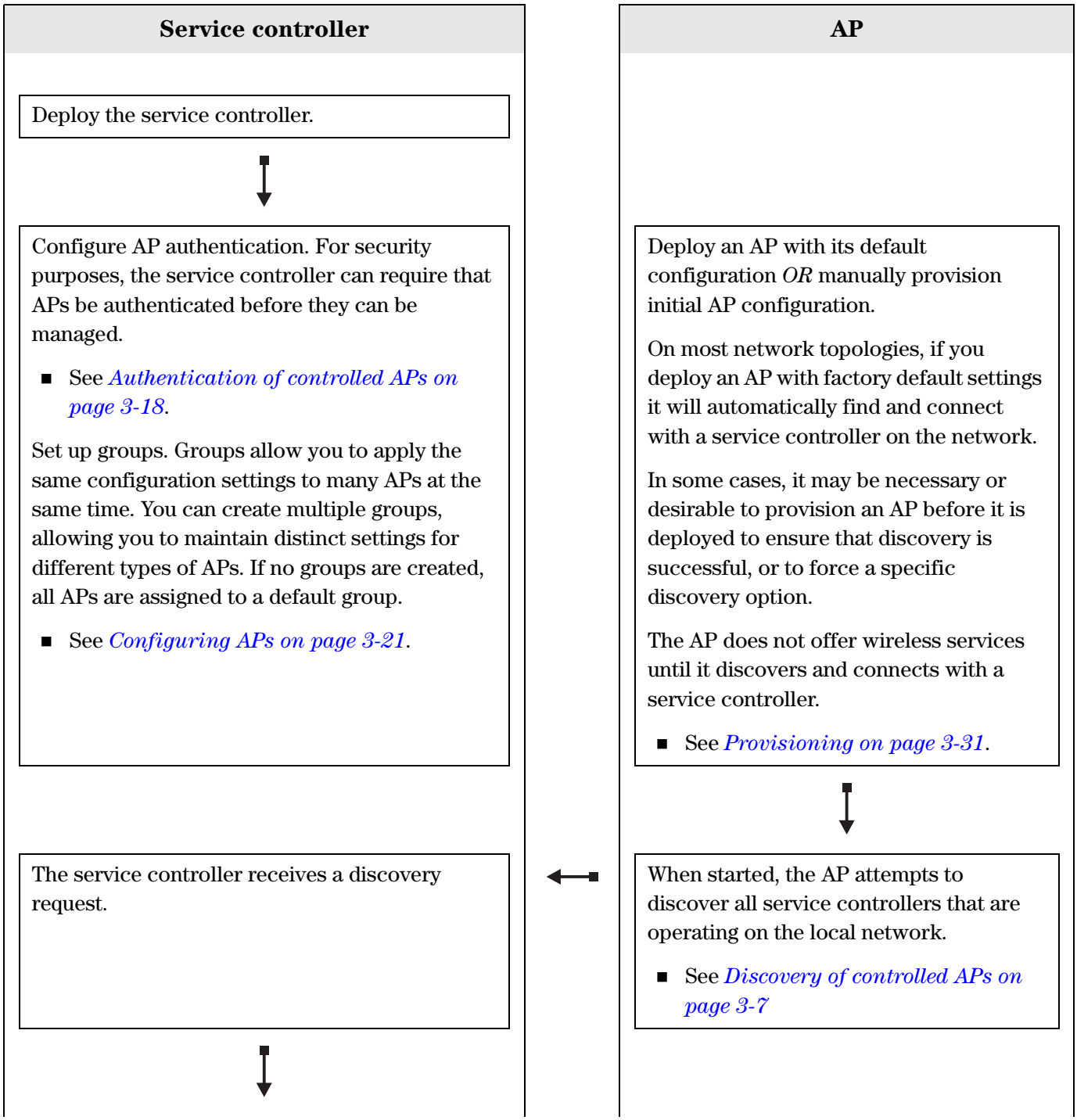
Once authenticated, a secure management tunnel is established between the AP and the service controller to support the exchange of management traffic between the two devices.

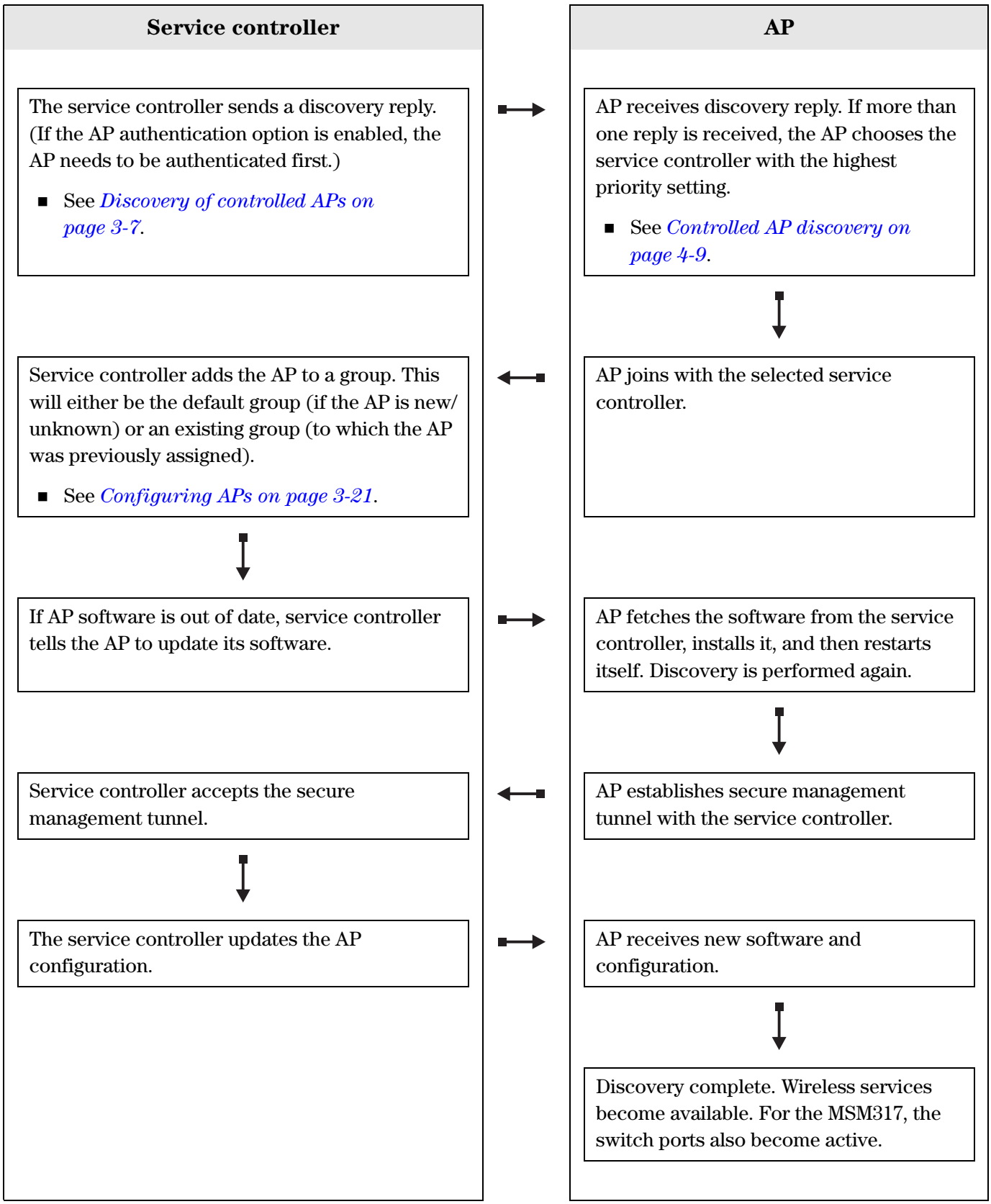
AP authentication

The service controller can be configured to authenticate APs by their MAC address before they are managed. The authentication can be defined locally on the service controller, via a third-party RADIUS server, or using a remote text-based control file.

Key controlled-mode events

The following diagram provides an overview of key events that occur when working with APs in controlled mode.


Service controller
AP
Deploy the service controller.
Configure AP authentication. For security purposes, the service controller can require that APs be authenticated before they can be managed.
See Authentication of controlled APs on page 3-18.
Set up groups. Groups allow you to apply the same configuration settings to many APs at the same time. You can create multiple groups, allowing you to maintain distinct settings for different types of APs. If no groups are created, all APs are assigned to a default group.
See Configuring APs on page 3-21.
Deploy an AP with its default configuration OR manually provision initial AP configuration.
On most network topologies, if you deploy an AP with factory default settings it will automatically find and connect with a service controller on the network.
In some cases, it may be necessary or desirable to provision an AP before it is deployed to ensure that discovery is successful, or to force a specific discovery option.
The AP does not offer wireless services until it discovers and connects with a service controller.
See Provisioning on page 3-31.
The service controller receives a discovery request.
When started, the AP attempts to discover all service controllers that are operating on the local network.
See Discovery of controlled APs on page 3-7


Service controller
AP
The service controller sends a discovery reply. (If the AP authentication option is enabled, the AP needs to be authenticated first.)
See Discovery of controlled APs on page 3-7.
AP receives discovery reply. If more than one reply is received, the AP chooses the service controller with the highest priority setting.
See Controlled AP discovery on page 4-9.
Service controller adds the AP to a group. This will either be the default group (if the AP is new/ unknown) or an existing group (to which the AP was previously assigned).
See Configuring APs on page 3-21.
AP joins with the selected service controller.
If AP software is out of date, service controller tells the AP to update its software.
AP fetches the software from the service controller, installs it, and then restarts itself. Discovery is performed again.
Service controller accepts the secure management tunnel.
AP establishes secure management tunnel with the service controller.
The service controller updates the AP configuration.
AP receives new software and configuration.
Discovery complete. Wireless services become available. For the MSM317, the switch ports also become active.

Discovery of controlled APs

This section describes how the discovery process works and how it can be customized.

Discovery is the process by which a controlled AP finds a service controller on a network and establishes a secure management tunnel with it. To see how the discovery process fits into overall controlled mode operations, see *Key controlled-mode events on page 3-5*.

In most cases, the factory default configuration of an AP will result in automatic discovery of a service controller with no configuration required. However, for some network topologies it may be necessary to configure the discovery process as described in this section.

See *Discovery recommendations on page 3-9* for examples of topologies that can use automatic discovery and those that require discovery to be configured.

Note

- If you intend to manage controlled APs via local mesh, see *Local mesh on page 13-1*.
- Provisioning can limit the discovery of potential service controllers. See *Provisioning on page 3-31*.

Discovery overview

Although the specifics of the discovery process vary depending on whether an AP is *unprovisioned* (in its factory default state) or *provisioned* (had its connectivity or discovery settings changed from their factory default settings), the discovery process can be summarized as follows:

1. The AP uses various methods to locate one or more service controllers that are reachable on the network. The preferred way to monitor AP discovery is via the service controller management tool (see *Monitoring the discovery process on page 3-13*). When in visual range of the APs, you can watch the status lights for an indication of discovery progress. See the status light information in the AP Quickstart (provided and available online).
2. Discovered service controllers send a discovery reply to the AP. If the service controller is configured to require AP authentication, the reply is only sent after the AP is authenticated by the service controller.
3. The service controller adds the AP to a group. This will either be the default group (if the AP is new/unknown) or an existing group (to which the AP was previously assigned).
4. The AP is now managed by the service controller, and it can be configured and monitored using the service controller management tool.

Note

- APs must be connected to the network via Port 1 (or the Uplink port on an MSM317) for discovery to work.
- Unprovisioned APs must obtain an IP address from a DHCP server before discovery can be initiated. When discovery occurs on a VLAN, the DHCP server must be active on the VLAN.

Discovery is performed whenever an AP:

- Is restarted (or reset to factory defaults),
- Loses connectivity with its service controller,
- Is removed and rediscovered using an action on the **Controlled APs >> Overview > Discovered APs** page.

Discovery methods

Four discovery methods are available. The following table summaries their features and recommended applications.

Method	Description	Supported by	Suggested use
UDP broadcast	AP issues UDP broadcasts to discover service controllers on the same subnet.	Unprovisioned APs	Both the service controller and AP reside on the same subnet.
DHCP	AP obtains service controller address from a specially configured DHCP server.	Unprovisioned APs	The AP is on a different subnet than the service controller.
DNS	AP obtains service controller address from a DNS server using predefined host names.	Unprovisioned APs Provisioned APs	The AP is on a different subnet than the service controller.
Specific IP addresses	AP connects to a specific service controller using a pre-configured static IP address.	Provisioned APs	DHCP and DNS are not used and the AP is on a different subnet than the service controller.

Note

A service controller listens for discovery requests on its LAN port and/or Internet port as configured on the **Service Controller >> Management > Device Discovery** page. (See *Device discovery on page 4-8*).

UDP broadcast discovery

The AP sends a UDP broadcast to discover all service controllers that are on the same subnet as the AP.

DHCP discovery

When configured as DHCP client (which is the factory default setting for all APs), an AP can obtain the IP addresses of service controllers on the network from any DHCP server configured to support the Colubris Vendor Class (DHCP option 43).

Vendor Class enables an administrator to define a list of up to three available service controllers on the network to which APs can connect.

- If the service controller is configured to operate as the DHCP server for the network, you can define the list of available service controllers by selecting **Service Controller >> Network > Address allocation > DHCP server** and then configure the **Service controller discovery** option.
- If an external DHCP server is used, it must have **Option 43** configured. For examples on how to configure some popular third-party DHCP servers, see *Appendix E: DHCP servers and Colubris vendor classes*.

DNS discovery

DNS discovery is attempted using UDP unicast discovery requests which are issued by the AP to the following default service controller names:

- cnsrv1
- cnsrv2
- cnsrv3

This method enables discovery across various network configurations. It requires that at least one service controller name is resolvable via a DNS server.

The AP appends the default domain name returned by a DHCP server (when it assigns an IP address to the AP) to the service controller name. For example, if the DHCP server returns **mydomain.com**, then the AP will search for the following service controllers in this order:

- cnsrv1.mydomain.com
- cnsrv2.mydomain.com
- cnsrv3.mydomain.com

Discovery using specific IP addresses

Provisioned APs can be configured to connect with a service controller at a specific IP address. A list of addresses can be defined, allowing the AP to search for multiple service controllers.

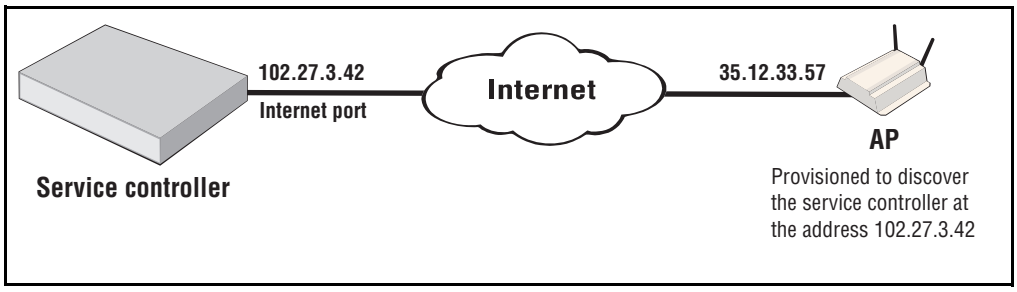
This can also be used to strengthen the security on a local network to make sure that the AP goes to a specific service controller for management.

Discovery recommendations

- **If the AP is on the same subnet as the service controller**, then UDP discovery will work with no configuration required on either the AP or service controller. This applies whether the service controller is operating as the DHCP server for the network or if a third-party DHCP server is used.

If VLANs are being used, then UDP discovery will also work with no configuration. However, to speed up the discovery process you can provision the AP with a specific VLAN ID. This will eliminate the need for the AP to find and attempt discovery on all available VLANs.

- **If the AP is on a different subnet than the service controller,** UDP discovery will not work. Instead, DHCP or DNS discovery must be used, or direct IP address discovery must be provisioned.
  - **DHCP discovery:** If you have control of the DHCP server, enable support for the Colubris Vendor Class as explained in *DHCP discovery on page 3-8*.
  - **DNS discovery:** If you have control of the DNS server, you can configure it to resolve the default service controller names that an AP will search for. To use custom names, you must provision discovery settings on the AP. For more information on using custom names, see *Provisioning discovery on page 3-36*.
  - **Specific IP discovery:** This method needs to be used when you do not have control over the DHCP and DNS servers and no domain is registered to the service controller. For example, if the connection to the service controller is routed over the public Internet.



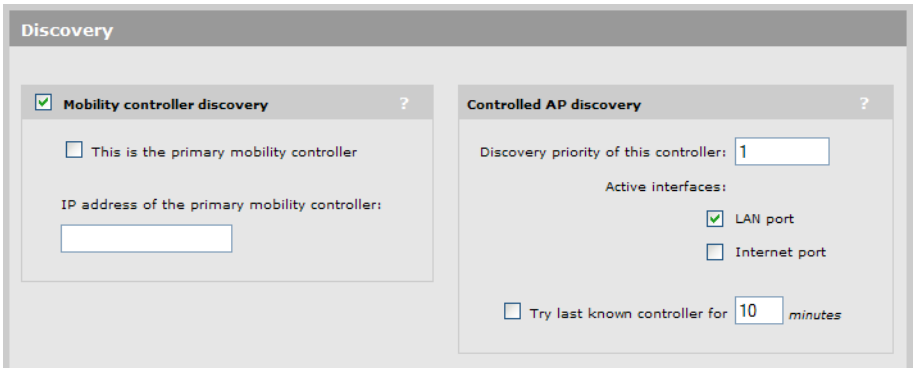
For discovery to succeed, the AP must be provisioned with the service controller IP address. See *Provisioning discovery on page 3-36*.

Discovery priority

Each service controller that receives a discovery request sends the requesting AP a discovery reply. If the AP authentication option is enabled, the AP needs to be authenticated first. Requests from unauthenticated APs are ignored.

If an AP receives discovery replies from multiple service controllers, the AP selects the service controller that has the highest discovery priority setting.

Discovery priority is set on a service controller using the **Discovery priority of this controller** option on the **Service Controller >> Management > Device Discovery** page.



If two service controllers have the same high-priority setting, the AP will appear on the **Overview > Discovered APs** page of both service controllers with a **Diagnostic** value of **Priority Conflict**. To resolve the conflict, change the priority setting of one of the service controllers on its Discovery page.

Discovery behavior

Discovery occurs differently for unprovisioned and provisioned APs.

Unprovisioned APs

Once an unprovisioned AP has received its IP address from a DHCP server (either from the service controller-based DHCP or the corporate DHCP), it attempts to discover a service controller using the following methods, in order:

- UDP broadcast
- DHCP
- DNS.

These discovery methods are applied on the following interfaces, in order:

- Last interface on which a service controller was discovered. (Only applies to APs that have previously discovered a service controller)
- Untagged on Port 1
- All other detected VLANs (in sequence) on Port 1.

Provisioned APs

The discovery method that is used depends on how the AP is provisioned. If discovery settings are provisioned, then the AP uses only the provisioned settings. The following discovery options are available:

- DNS discovery: Enables custom service controller names and domains to be used for discovery.

- Discovery using an IP address: Enables the AP to find service controllers operating at a specific IP address.

If only connectivity settings are provisioned, then the AP attempts to discover a service controller using the same methods as for unprovisioned APs, namely:

- UDP broadcast
- DHCP (the AP must be configured as a DHCP client for this to work)
- DNS

Tip

For more information on provisioning APs, see *Provisioning on page 3-31*.

Discovery considerations

The following considerations must be made with respect to discovery:

Firewall

If the network path between an AP and a service controller traverses a firewall the following ports must be opened for management and discovery to work:

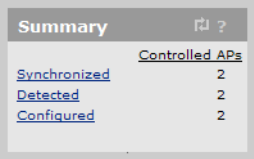
Protocol	Open these ports	Ports are used by
UDP	Source and destination = 38212 (9544 hex).	Discovery protocol the AP uses to find a service controller.
UDP	Destination = 1194 (4AA hex).	Management tunnel that is established between an AP and a service controller.
TCP	Source and destination = 1194 (4AA hex).	Software updates and certificate exchanges (for the management tunnel).
UDP	Source and destination = 3001 (BB9 hex).	Client data tunnel.
UDP	Source = 39064 (9898 hex) and destination = 1800 (708 hex), 1812 (714 hex), 1813 (715 hex), 30840 (7878 hex).	Location aware. This is only necessary if autonomous APs are using the access-controlled (public access) interface.

NAT

If the network path between an AP and a service controller implements NAT (network address translation), discovery will only work if NAT functions on outbound traffic sent from the AP to the service controller. If NAT operates in the other direction, discovery will fail.

Monitoring the discovery process

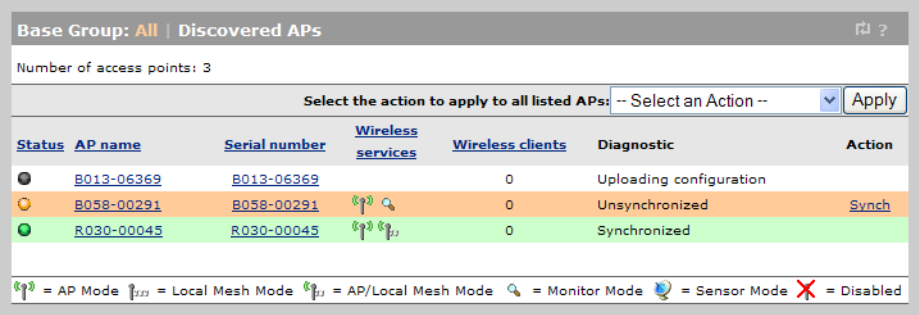
This Summary menu lists the number of controlled APs discovered by the service controller. APs are grouped according to their management state. For example: **Synchronized**, **Detected**, **Configured**, **Pending**.



An AP may be active in more than one state at the same time. For example, an AP may be both **Detected** and **Synchronized**. Select the state name to display information about all APs in that state.

Viewing all discovered APs

To display information about APs discovered by the service controller, select **Controlled APs >> Overview > Discovered APs**.


Base Group: All | Discovered APs
Number of access points: 3
Select the action to apply to all listed APs: -- Select an Action -- Apply
Status AP name Serial number Wireless services Wireless clients Diagnostic Action
B013-06369 B013-06369 0 Uploading configuration
B058-00291 B058-00291 0 Unsynchronized Synch
R030-00045 R030-00045 0 Synchronized
= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Sensor Mode = Disabled

The **Discovered APs** page provides the following information:

- **Number of access points**: Indicates the number of APs that were discovered.
- **Select the action to apply to all listed APs**: Lets you apply the selected action to all APs in the list. Select an action and then **Apply**.
- **Status:**
  - Green: The AP is synchronized, meaning that the AP is connected, running, and has received its configuration from the service controller.
  - Yellow: The AP is unsynchronized, meaning that the AP is operational but does not have the same configuration as the service controller, yet.
  - Red: The AP is not part of the controlled network and is not providing wireless services. See the **Diagnostic** column for details.
  - Grey blinking: An action is pending.
  - Grey: The AP is configured in a group, but has not been discovered on the network.
- **AP name**: Name assigned to the AP.

- **Serial number**: Unique serial number assigned to the AP at the factory. Cannot be changed.
- **Wireless services**: Indicates the status of wireless services on the AP. A separate icon appears for each radio on the AP. See the legend under the table for the meaning of each icon.
- **Wireless clients**: Indicates the number of wireless clients currently associated with the AP. Select the number to see more information.
- **Diagnostic**: Indicates the status of the AP with regards to management by the service controller, as shown in the following table.

Diagnostic	Description
Waiting for acceptance	The AP has been authorized by the service controller. However, the AP has not yet selected the service controller to function as its service controller. (If multiple service controllers replied to the APs discovery request, the AP may choose to connect with another service controller.)
Priority conflict	More than one service controller responded to the AP discovery request with the same priority. The AP is therefore unable to select a service controller to function as its service controller. The AP will retry its discovery request shortly. You must fix the priority conflict by changing the priority setting for one of the service controllers (**Service Controller >> Management > Device discovery**).
Not authorized	The AP could not be authenticated by the service controller. This may be due to invalid authentication credentials supplied by the AP. Authentication settings used by the service controller are defined on the **Service Controller >> Authentication** page. You should accept the AP unless it is an actual rogue.
Not responding	The AP has stopped sending management information to the service controller. Rediscovery may re-establish the connection. If not, the AP may have lost power or a network failure has occurred.
Wrong Product	The AP was created with a product type that does not match the detected product type. This can occur when an AP is manually added to a group with the wrong product type. For example, an MSM310 was added as an MSM320. You should verify and fix the product type.

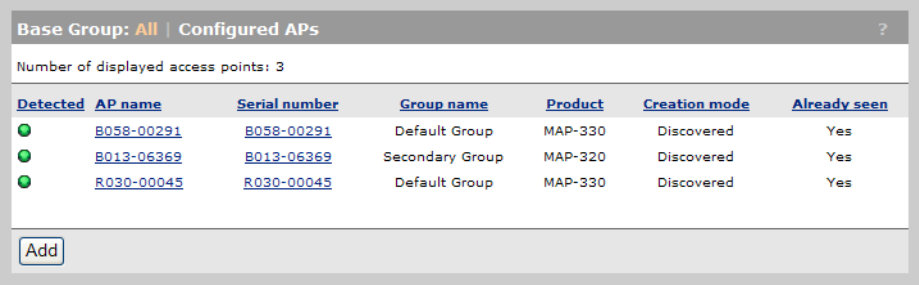
Diagnostic	Description
Unconfigurable	This AP cannot be added because the maximum number of configured APs has been reached. To add this AP you must first remove one or more currently configured APs.
Validating firmware	The service controller is waiting for the AP to send its software version number.
Uploading firmware	The service controller is uploading new software to the AP. Wait until the operation completes.
Installing firmware	New software has been successfully uploaded to the AP. Wait until the AP restarts to activate the new software.
Firmware failure	New software failed to upload to the AP. The service controller will retry soon.
Unsupported product	No suitable software is available for this AP on the service controller. You should update the service controller software so that the newly-introduced product can be recognized.
Establishing tunnel	A secure management connection is being established to the AP.
Suspicious device	These AP has unexpectedly requested a new authentication certificate from the service controller. Possible causes are: ■ A previously synchronized AP was reset to factory defaults. ■ An unauthorized AP may be using the same MAC address. This is a possible security breach that should be investigated before authorizing the AP again.
Validating configuration	The service controller is waiting for the AP to send its configuration.
Uploading configuration	Configuration settings are currently being sent to the AP.
Synchronized	The AP is up and running, offers wireless services, and had its software and configuration settings successfully updated by the service controller.
Unsynchronized	The AP is up and running and offers wireless services. However, its configuration settings do not match the settings defined on the service controller (at the group or AP level). You should Synchronize the AP.

Diagnostic	Description
Resetting configuration	The AP configuration is being reset to factory defaults. This is normal and will occur when the software version on the service controller is changed or if the AP is not synchronized.
Validating capabilities	The capabilities of the AP are being identified by the service controller.
Invalid country	The AP cannot be configured with the current country settings defined on the service controller. This can occur when an AP manufactured for use in a specific country is deployed in another country. You should replace the AP with one configured for the same country as the service controller.
Restoring configuration	The AP is currently restoring its previous configuration settings.
Rebooting	The AP is restarting.
Synchronized/License violation	Although the AP is synchronized it is non-functional (quarantined) due to a license violation. You must change the configuration to omit the affected licensed feature or acquire and install a valid license.
Unsynchronized/License violation	The AP is not synchronized but can continue operation. However, if synchronized, it will become non-functional as described above for Synchronized/License violation. Before synchronizing, either change the configuration to omit the affected licensed feature or acquire and install a valid license.
Incompatible settings	Local mesh has been provisioned on the AP but: ■ The APs radio is disabled. ■ The AP radio operating mode does not support local mesh. ■ The APs radio wireless mode does not match the one provisioned. ■ The mesh ID is not uniquely assigned. Click on the **Incompatible Settings** link for a detailed description.
Enabling VSC services	The AP is enabling wireless services for all VSCs.
Detected	The AP was detected by the service controller.

- **Action**: Indicates the recommended administrative action to be taken to resolve a diagnostic condition.

Viewing all configured APs

To display information about APs configured by the service controller, select **Controlled APs >> Overview > Configured APs**.



The **Configured APs** page provides the following information:

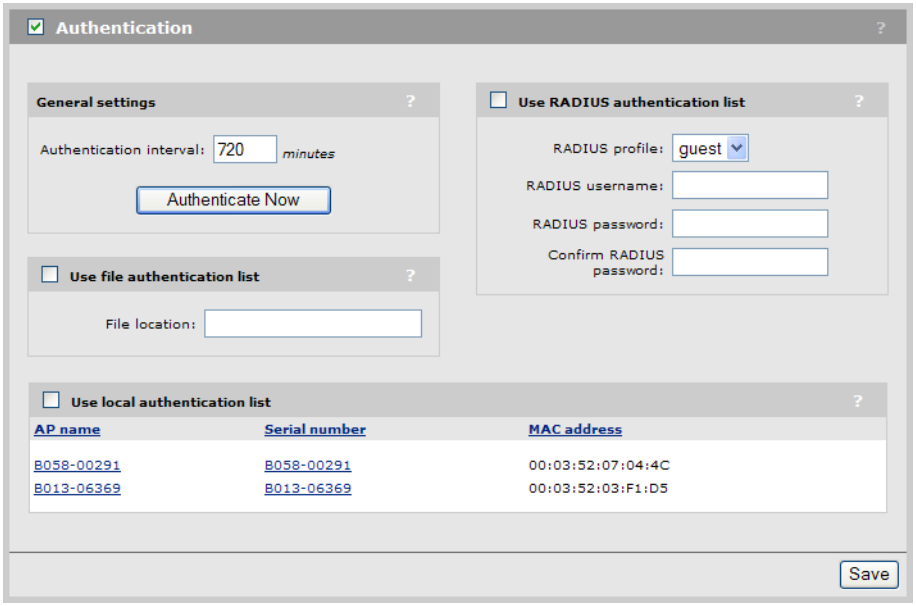
- **Number of displayed access points**: Number of configured APs that were discovered.
- **Detected**: Status light icon indicating if the AP has been detected.
  - Green: The AP has been discovery and is listed on the AP overview page, where more information is provided on the AP.
  - Red: The AP has not been discovered.
- **AP name**: Name assigned to the AP. Select the name to open its AP management page.
- **Serial number**: Serial number assigned to the AP. Select the serial number to open its AP management page.
- **Group Name**: Group that the AP is part of.
- **Product**: Product name of the MSM AP.
- **Creation mode**:
  - **Local**: AP was added manually, or was manually authenticated after being discovered.
  - **RADIUS**: AP was successfully authenticated via RADIUS and then created.
  - **External file**: AP was successfully authenticated using the external file option.
  - **Discovered**: Automatically detected by the service controller based on discovery-time parameter exchange.
- **Already Seen**: The AP established a management tunnel to the service controller at least once in the past.

Authentication of controlled APs

For security purposes, the service controller can require that APs be authenticated before they are managed. Authentication is enabled by selecting **Service controller >> Controlled APs > Authentication.**

Note

The AP authentication option is disabled by default, meaning that all discovered APs are authorized (no authentication is required).



The service controller authenticates APs using their MAC addresses. When an AP sends a discovery request to the service controller, it includes its Ethernet Base MAC address. The service controller validates this address against its AP address authentication list. If the address appears in the list, the AP is authenticated and gains access to the service controller's service control features.

If authentication fails (for example, this is a new AP), and the **Use the local authentication list** option is enabled, then the AP is added to the **Default Group** and flagged as requiring authentication. The AP must then be manually authenticated by a manager using the **Controlled APs >> Overview > Discovered APs** page. Once authenticated, the AP can be managed.

Note

APs remain visible in this list as long as they have been detected and authorized at least once. If an AP is no longer part of the network then a manager must manually remove it.

Building the AP authentication list

The service controller can retrieve authentication list entries from several sources: a RADIUS account, a file, or using the set of locally configured APs. All entries are merged to create a combined list.

The service controller retrieves authentication list entries when:

- The **Authentication interval** expires
- **Authenticate Now** is clicked
- **Save** is clicked
- Each time the service controller starts up.

Each time the authentication list entries are retrieved, all connected APs are checked against it. If an AP MAC address is no longer listed, its connection is terminated.

Note Although the same RADIUS account can be shared between this option and the **Public access > Attributes** page, it is recommended that a separate RADIUS account be created for each option.

General settings

Authentication interval

Specifies the interval at which the service controller retrieves authentication list entries from the selected authentication sources. After the entries are retrieved all controlled APs are evaluated against the new list.

Authenticate Now

Causes the service controller to retrieve authentication list entries from all selected sources.

Use file authentication list

When this option is selected, the service controller retrieves authentication list entries from a file. This must be an ASCII file with one or more MAC addresses in it. Each address must be entered on a separate line. For example:

```
00:03:52:00:00:01
00:03:52:00:00:02
00:03:52:00:00:03
```

A label affixed to each AP indicates its Ethernet Base MAC Address. This is the address to specify in the authentication list.

File location

Specify the location of the file to use for authentication of APs using either HTTP or FTP. For example:

ftp://mydomain.com/auth_list
ftp://*username*:*password*@mydomain.com/auth_list
http://mydomain.com/auth_list

Use RADIUS authentication list

When this option is selected, the service controller retrieves authentication list entries from a RADIUS server. List entries must be defined in the RADIUS account for the service controller using the following Colubris-AVPair value string:

`managed-ap=`*MAC_address*

Where *MAC_address* is the Ethernet Base port MAC address of the controlled AP (which is printed on a sticker affixed to the AP case). Use colons to separate characters in the address.

For example: `00:20:E0:6B:4B:44`.

To define multiple addresses, specify additional entries as needed.

This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server if it is not already present as follows:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type = string

RADIUS profile

When the **Authentication** source is **RADIUS**, this option specifies the name of the RADIUS profile to use. There is no default. To configure RADIUS profiles, select **Service Controller >> Authentication > RADIUS profiles**.

RADIUS username

When the **Authentication** source is **RADIUS**, specifies the RADIUS username assigned to the service controller.

RADIUS password / Confirm RADIUS password

Specifies the password that corresponds with **RADIUS username**.

Use the local authentication list

When this option is selected, the service controller creates authentication list entries based on the set of APs that are currently defined on the service controller. For reference purposes, the table shows the **AP name**, **Serial number** and **MAC address** of all APs that are defined and will be included in the authentication list.

Note

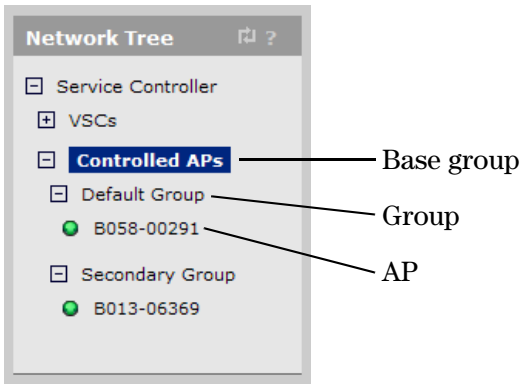
When the local authentication list is enabled, the first time an AP tries to connect to the service controller, a manager must manually accept the AP on the **Controlled APs >> Overview > Discovered APs** page. Otherwise, the AP will not be able to connect to the service controller.

Configuring APs

This section explains how to configure APs using the Controlled APs menu in the Network Tree.

Overview

To make the configuration of multiple APs easier to manage, parameters settings are managed using a hierarchal structure, where the configuration settings at lower levels are inherited from those at higher levels. There are three levels to the hierarchy: base group, group, and AP. For example:



- Click the **+** symbol next to **Controlled APs** to expand the tree to see all groups.
- Click the **+** symbol next to each group to see its APs.

The levels are defined as follows:

- **Base group:** The base group is called **Controlled APs**. This name cannot be changed and you cannot create an additional base group.
- **Group:** Group-level configuration enables you to define settings that are shared by APs with similar characteristics. For example, if you have several APs at a location that are all providing the same service, putting them in the same group makes them easier to manage. The **Default Group** is always present. All newly-discovered APs are initially placed into this group. You can create multiple groups.
- **APs:** AP-level configuration enables you to specify configuration settings for a particular AP that overrides corresponding group-level settings.

Note

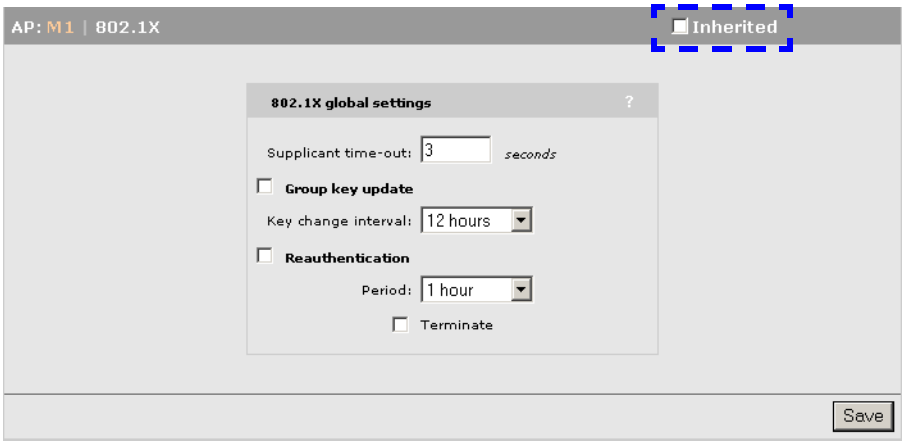
Assignment of VSCs can only be done at the group level. This means that all APs in a group always have the same VSC settings. The only exception to this is the MSM317 which allows VSCs to be bound to individual ports on its integrated switch. See the *MSM317 Access Device Installation and Getting Started Guide*.

Inheritance

Configuration settings are inherited as follows:

- Settings made at the **Controlled APs** level are inherited by all groups.
- Settings made at the **Group** level are inherited by all the APs in a group.

To change inherited configuration settings you must first clear the **Inherited** checkbox. For example, the following image shows the **802.1X** page with the **Inherited** checkbox cleared, allowing all settings on this page to be customized.



Binding VSCs to groups

The service controller defines a global pool of VSCs (*Working with VSCs on page 2-1*) that represents the services that are available. From this pool, specific VSCs can be *bound* to one or more groups (and the APs in the groups), to define the features that will be offered throughout the wireless network.

Any changes to a bound VSC affect all groups (and APs) to which the VSC is bound, making it easy to manage configuration changes network-wide.

Note

On the MSM317, VSCs can also be bound directly to the switch ports. See the *MSM317 Access Device Installation and Getting Started Guide*.

Synchronizing APs

After making configuration changes to an AP or a group, you must update all affected controlled APs with the new settings by synchronizing them. See *Synchronizing APs on page 3-27*.

Configuration strategy

There are two ways to approach AP configuration:

Discover APs and then configure groups

This strategy works as follows:

1. Deploy the APs in their default configuration on the network.
2. Allow the discovery process to find the APs and place them in the default group.
3. Create group definitions and then move the APs to the appropriate group.

Tip

Configure the default group to disable all radios. In this way, the default group becomes a staging area to hold newly added APs. Once discovered, the new AP can be moved to its appropriate group where its radio is activated.

Configure groups and then discover APs

This strategy works as follows:

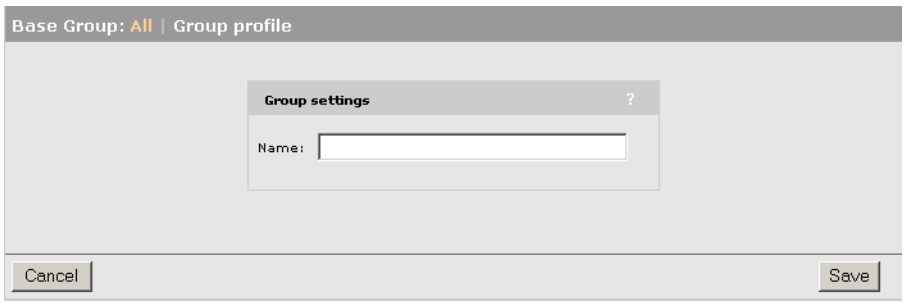
1. Create group definitions.
2. Manually define each AP in the appropriate group.
3. Deploy the APs in their default configuration on the network.
4. Allow the discovery process to find the APs and place them in the pre-configured groups.

Working with groups

Adding a new group

To create a new group, do the following:

1. Select **Controlled APs >> Group management**.
2. Select **Add New Group**.
3. Specify the name of the new group and select **Save**.



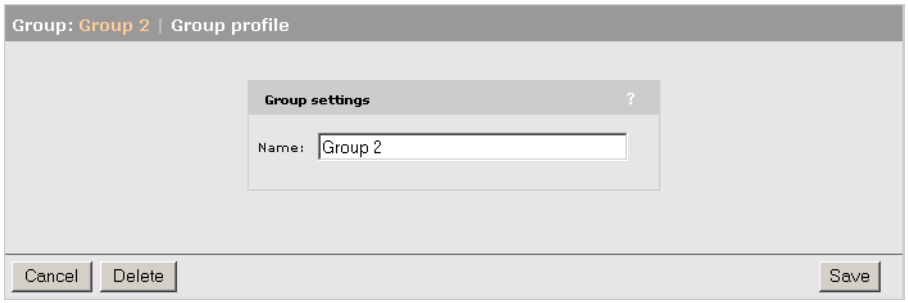
Deleting a group

Note

You must remove all APs from a group before you delete it.

To delete a group, do the following:

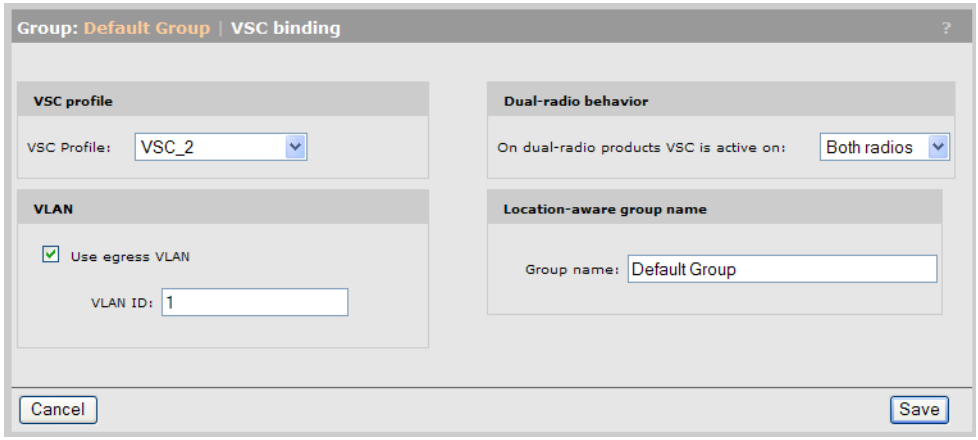
1. Select **Controlled APs >> Group management**.
2. Select the name of the group you want to delete.
3. Select **Delete**.



Binding a VSC to a group

To bind a VSC to a group, do the following:

1. Select the target group under **Controlled APs**.
2. In the right pane, select **VSC bindings**, then select **Add New Binding**.



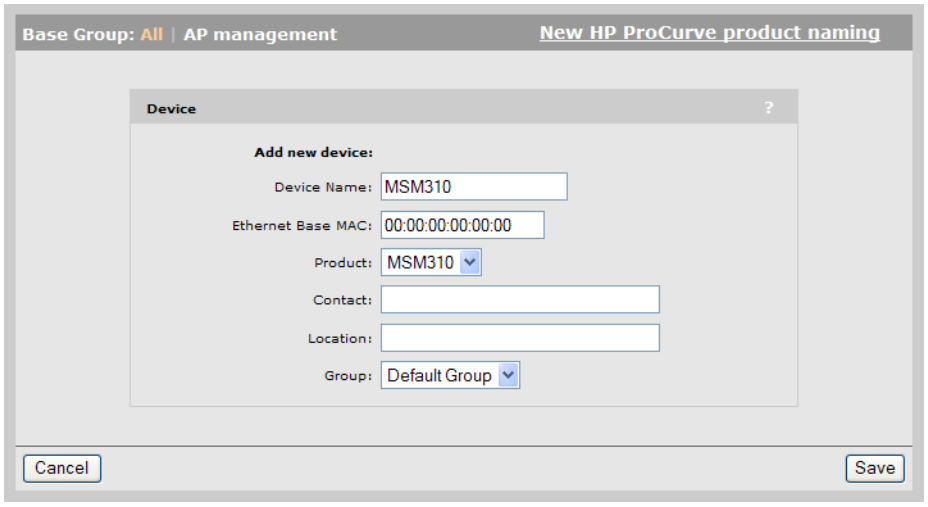
3. Select the **VSC profile** and define other configuration settings as required.
4. Select **Save**.

Working with APs

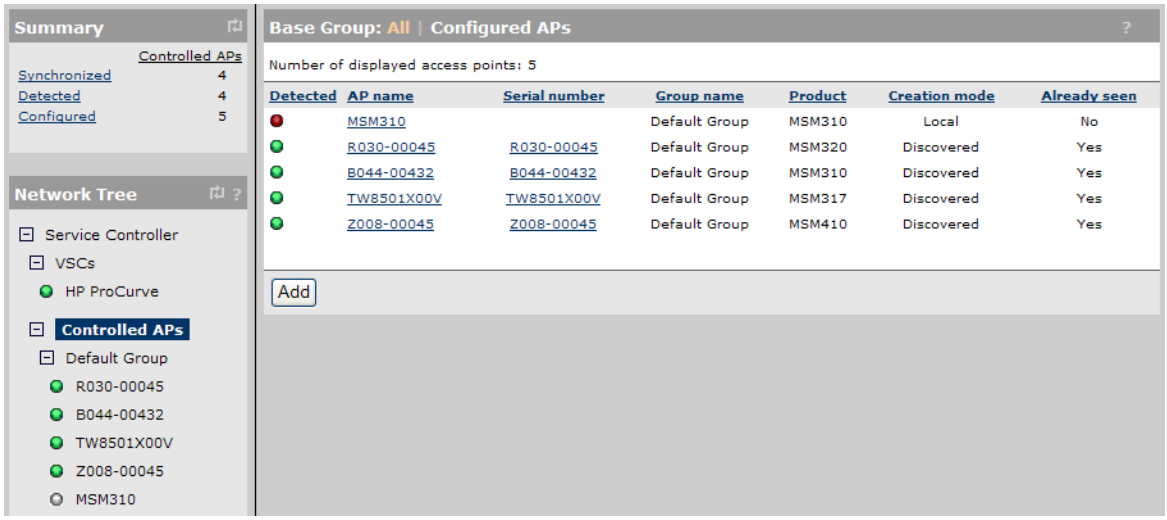
Manually adding a new AP

You can manually add APs to the service controller before connecting the APs to the network. This is useful, for example, when you want to pre-designate the group into which an AP will be placed.

1. Select **Controlled APs >> Overview > Configured APs**.
2. Select **Add**.
3. In the **Device** box, identify the new AP, specifying at a minimum, **Device Name**, **Ethernet BASE MAC** (printed on the label affixed to each AP), and **Group**.



Select **Save**. The AP is added to the selected group in the Network tree and will also be shown in the Configured APs list.



Note

- When the AP is physically connected to the network, it will discover the service controller and automatically be accepted into the selected group. Make sure you configure the correct MAC address, otherwise the AP will just be discovered as a new AP and will not be placed into the selected group.
- If an AP is created with the wrong product type it will go into the **Wrong product** state when discovered. (For example, if you specify MSM310 for an AP that is an MSM320.) To remedy this, select **Overview > Discovered APs** and select the **Accept Products** link in the **Action** column. (This action will override the pre-configured product setting by the information discovered from the actual physical AP.)

Deleting an AP

Note

When the AP authentication feature is disabled, a deleted AP may automatically rediscover the service controller if the AP is left connected to the network. Therefore, before deleting, disconnect the AP unless you want it to rediscover the service controller.

1. To delete an AP, select the AP in the **Network tree**, and then in the **Configured APs** list, select the AP name in the **Link** column.
2. On the **AP management** page, select **Delete**. The AP is deleted.

Moving an AP to a different group

Note

Moving an AP to a different group causes it to be restarted.

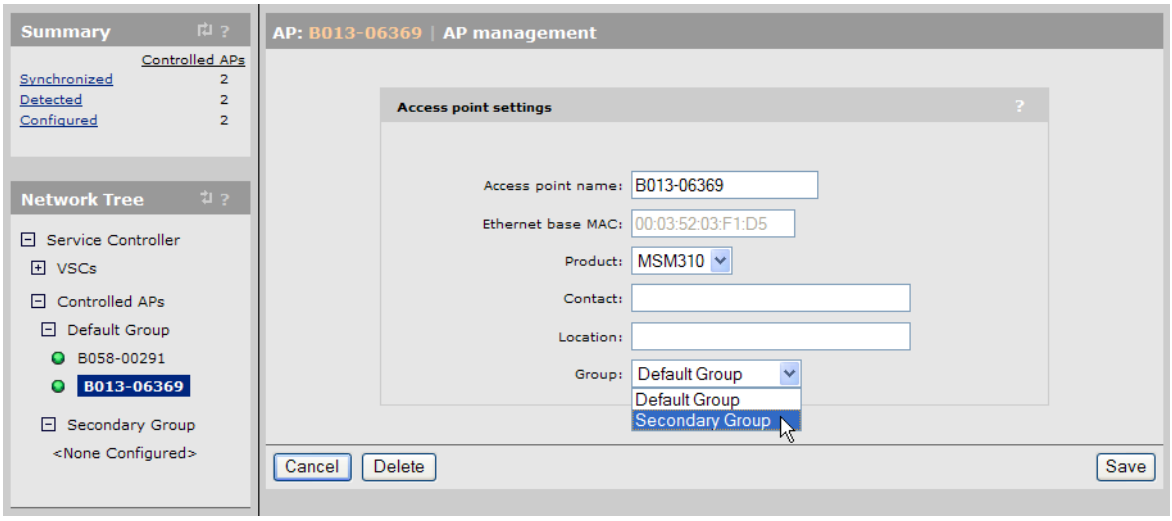
Using drag-and-drop

The easiest way to move an AP to a different group is to drag-and-drop it from the old group to the new group. Both groups must be visible in the Network tree for this to work.

The move to the different group does not actually occur until the AP is synchronized as described in the next section, *Synchronizing APs on page 3-27*.

Using menus

1. In the **Network tree** select the AP and then on the main menu, select **Device Management > AP management**.
2. Under Access point settings, select the desired **Group** and select **Save**.



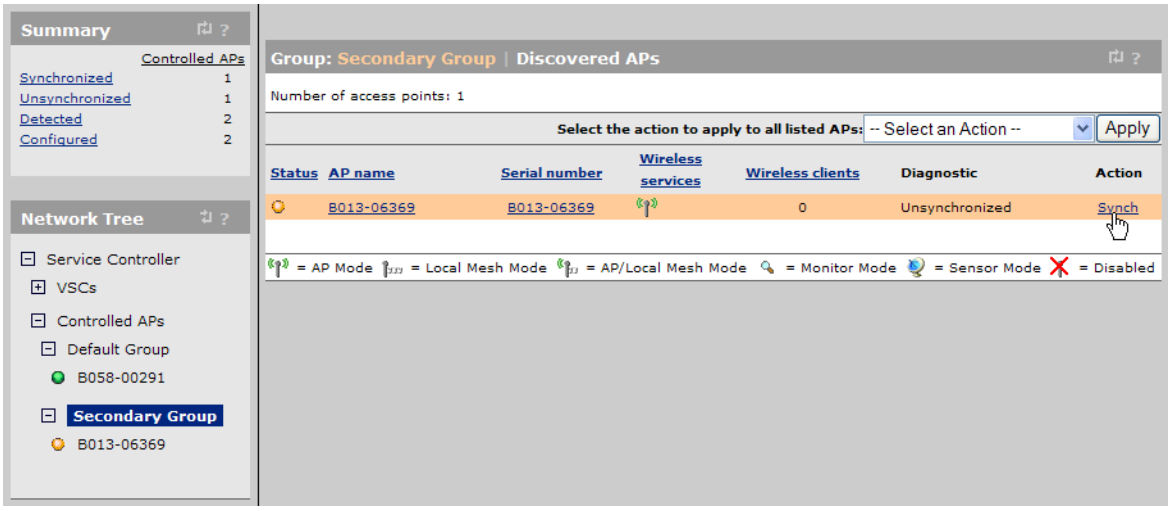
This puts the AP into the unsynchronized state (it will be displayed in orange). The move does not occur until the AP is synchronized as described in the next section.

Synchronizing APs

Depending on the type of configuration changes that are being synchronized, wireless users may be forced to reassociate or log in again.

After making configuration changes, you must synchronize the APs with the updated configuration as follows:

1. In the **Network tree**, select the group that contains the APs, and then in the right pane, select **Discovered APs**. For example, **Secondary Group**.

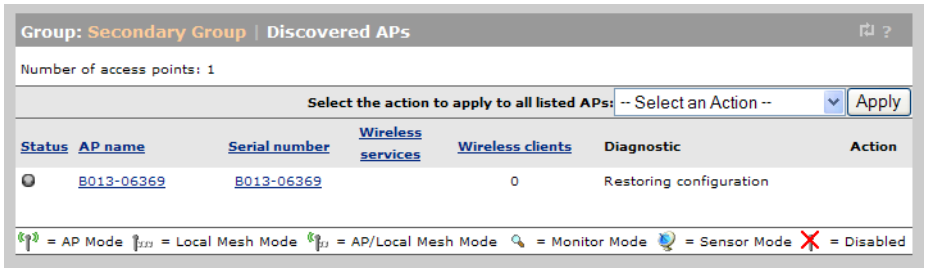


APs requiring synchronization are displayed with an orange background and show **Unsynchronized** in the **Diagnostic** column.

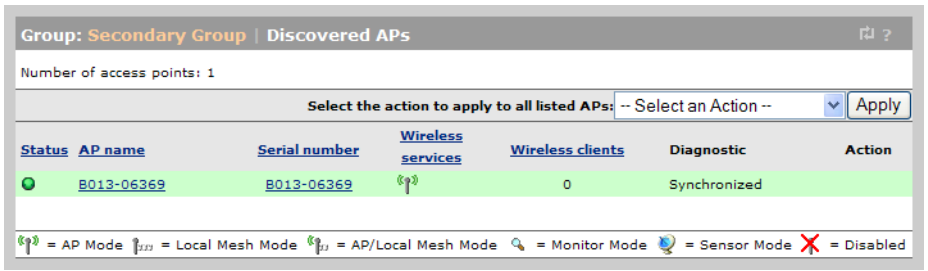
2. Select a **Synch** link in the **Action** column to synchronize a single AP.

   Or, to synchronize all unsynchronized APs in the group, select **Synchronize Configuration** in the **Select the action to apply to all listed APs** list, and select **Apply**.

3. Monitor synchronization progress by watching the **Diagnostic** column. Messages such as **Resetting configuration** and **Restoring configuration** will appear during the synchronization process.


Group: Secondary Group | Discovered APs
Number of access points: 1
Select the action to apply to all listed APs: -- Select an Action -- Apply
Status AP name Serial number Wireless services Wireless clients Diagnostic Action
B013-06369 B013-06369 0 Restoring configuration
= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Sensor Mode = Disabled

4. As each synchronization completes, the **Status** light icon and background color of the synchronized AP changes to green. The status light icon next to the AP name under the pertinent group name in the Network tree also changes to green. This indicates that the AP is fully operational and using its new configuration.


Group: Secondary Group | Discovered APs
Number of access points: 1
Select the action to apply to all listed APs: -- Select an Action -- Apply
Status AP name Serial number Wireless services Wireless clients Diagnostic Action
B013-06369 B013-06369 0 Synchronized
= AP Mode = Local Mesh Mode = AP/Local Mesh Mode = Monitor Mode = Sensor Mode = Disabled

Defining VLANs

This section describes how to assign an egress VLAN to controlled APs. All traffic from wireless users will be forwarded to the service controller on the specified VLAN.

- To define VLANs on an MSM317 switch port, see the *MSM317 Installation and Getting Started Guide*.
- For information on the service controller VLAN implementation, see *VLAN support on page 10-11*.

Each time a VSC is bound to a group, you have the option of assigning a VLAN ID to be used for egress traffic sent by all APs in the group. For example, if VSC 1 and VSC 2 are both bound to the Default Group, the egress traffic for each VSC could be tagged with a different VLAN to segregate the traffic.

Note

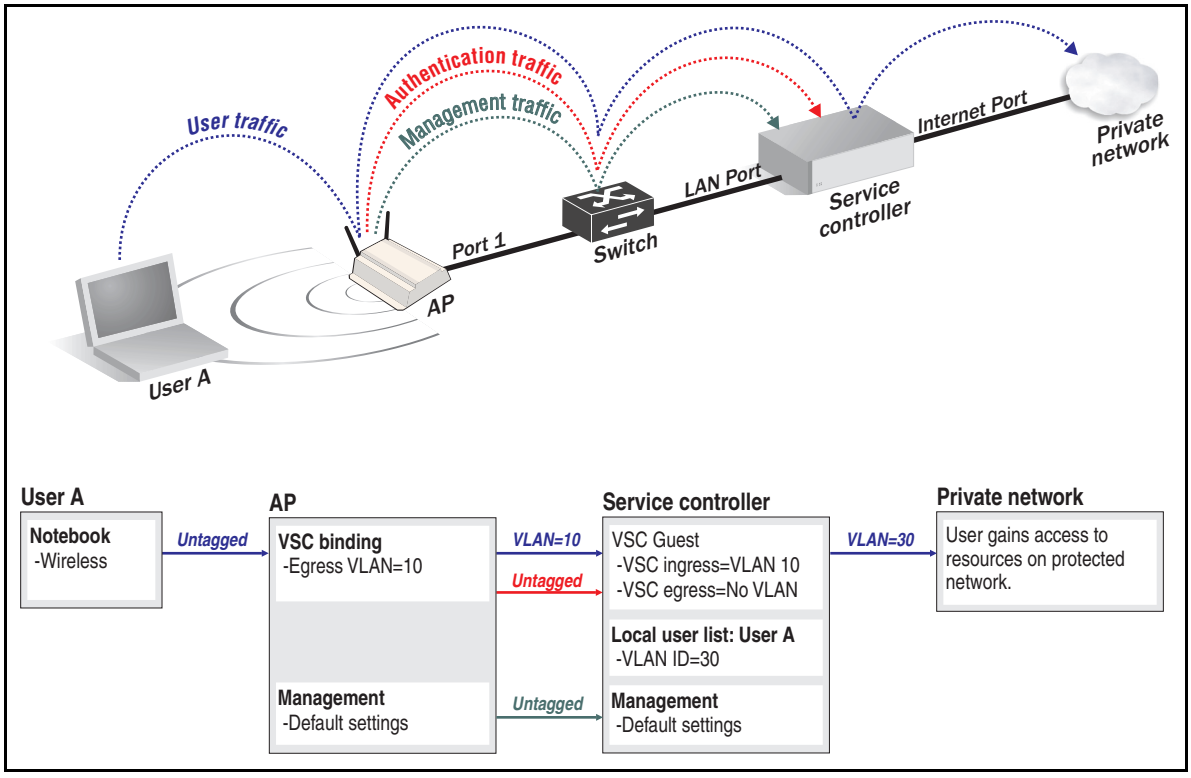
If an access-controlled VSC is bound to a group, the VLAN must match the ingress VLAN on the VSC (or be altered by a switch between the AP and the service controller to do so.).

Dynamic VLANs

When a dynamic VLAN is assigned to a user, it overrides the egress VLAN set here as follows:

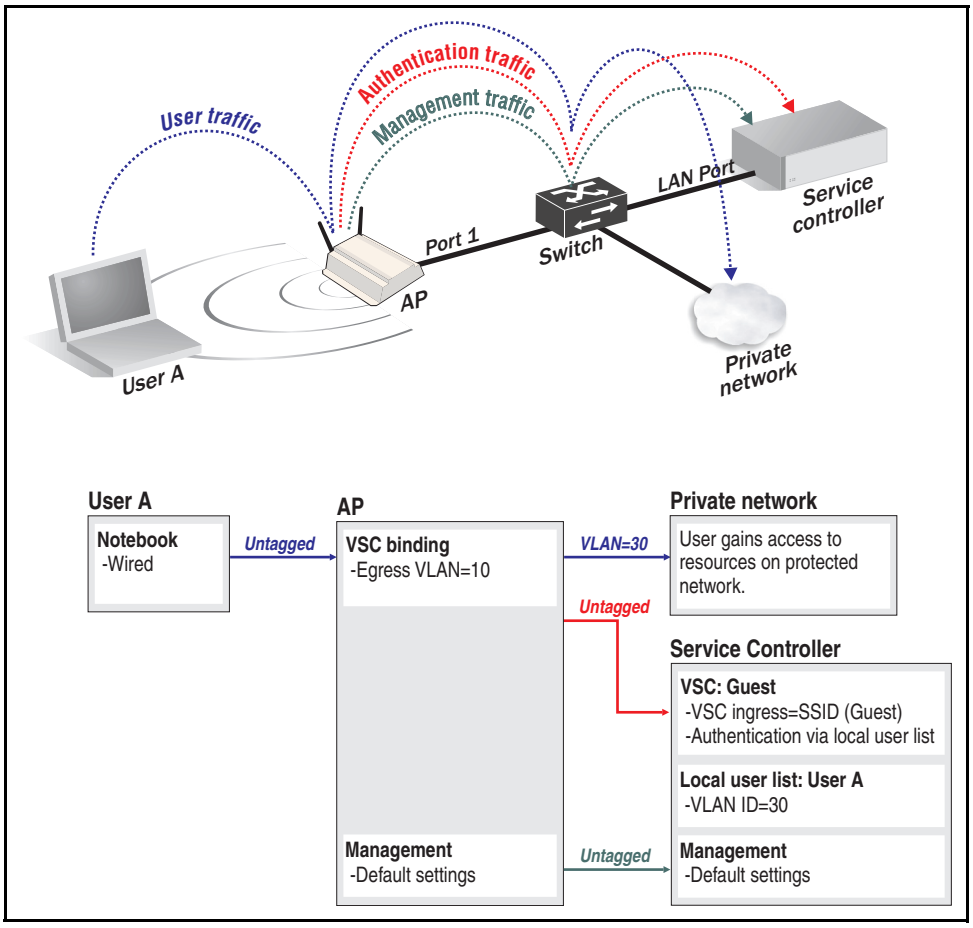
- If the group is bound to an access-controlled VSC, the dynamic VLAN applies on the service controller and overrides the **VSC egress mapping** on the bound VSC.

  For example, if **Use egress VLAN** is set to 10, the AP sends traffic to the service controller on VLAN 10. This traffic is picked up by the VSC with Ingress set to 10. Now if a dynamic VLAN of 30 is assigned to the user, then the egress traffic on this VSC for the user occurs on VLAN 30 (regardless of the egress setting for the VSC). So user traffic exits the service controller on VLAN 30.



- If the group is bound to an non-access-controlled VSC, the dynamic VLAN applies on the AP resulting in user traffic being sent from the AP tagged with the dynamically assigned VLAN.

  For example, if **Use egress VLAN** is set to 10, and a dynamic VLAN of 20 is assigned to the user, then the AP sends outgoing traffic for this user on VLAN 20.



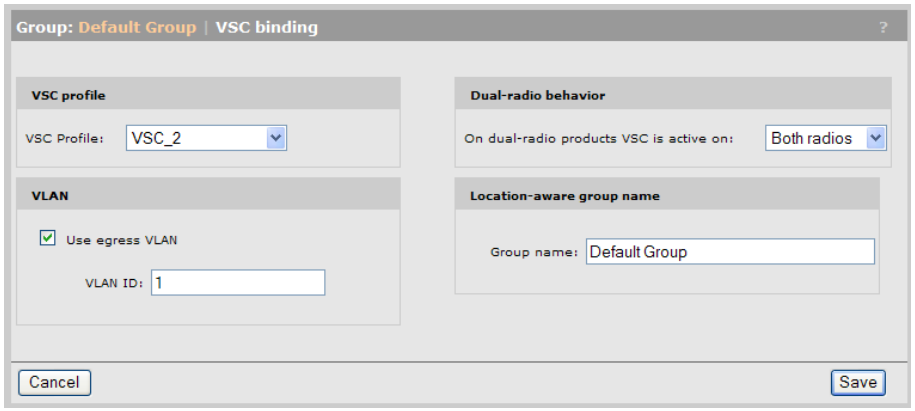
Dynamic VLANs are assigned by setting an attribute in a user's RADIUS account or in a local user account.

To define a VLAN

Define an egress VLAN as follows:

1. Select the target group under **Controlled APs**.
2. In the right pane, select **VSC bindings** and then select a binding in the list.

3. Select the **Use egress VLAN** checkbox and then specify a **VLAN ID**.



4. Select **Save**.

Provisioning

Provisioning is the means by which you can change the factory default IP addressing method and service controller discovery settings on controlled APs.

Provisioning is generally not required when deploying controlled APs in simple network topologies. However, it is required when controlled APs:

- Do not have layer 2 connectivity to a service controller and where it is not possible to control the DNS or DHCP server configuration. See *Discovery recommendations on page 3-9*.
- Need to be deployed with static IP addresses.
- Use a local mesh to connect to the service controller. See *Provisioning local mesh links on page 13-12*. This feature is not supported on the MSM317.
- To accelerate the discovery process on networks with a large number of VLANs, or when many VLANs are connected to many service controllers.

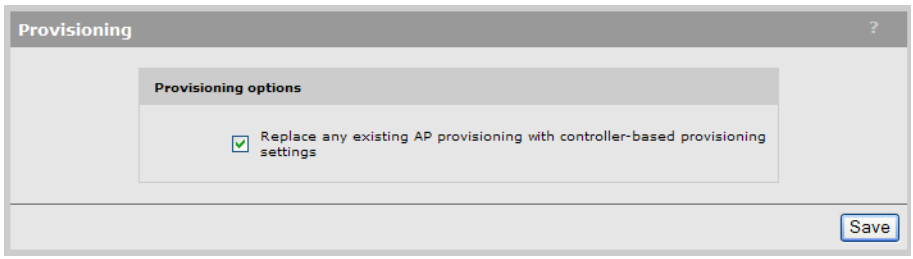
Provisioning methods

Provisioning can be done in two ways:

- **Use the service controller to provision controlled APs:** On the service controller, provisioning can be done at the group or AP level for added flexibility. Provisioning via the service controller is the preferred method.

  In certain scenarios it may be practical to use one service controller to provision APs, and then have the APs associate with another service controller after being deployed. For example, provisioning could occur at the network operations center by connecting APs to the same subnet as a service controller. Once provisioned, the APs can then be deployed in the field where they will discover a service controller already in operation.

To enable a service controller to send provisioned settings to controlled APs, you must first activate the **Enable provisioning of controlled APs** option on the **Service Controller >> Controlled APs > Provisioning** page.



Note

Until this option is enabled, provisioned settings defined on the service controller are not sent to any controlled APs.

After an AP has been updated with provisioned settings, these settings do not become active until the AP is restarted, or a **Remove and rediscover** action is executed on the **Controlled APs >> Configured APs** page.

- **Directly provision an AP using its management tool:** In its factory default state, the AP provides a provisioning menu with the same options that are available on the service controller. Use this method when there is no local service controller on which to perform the provisioning.

Note

Once an AP has established the secure management tunnel with a service controller, the provisioning menu on the AP is no longer accessible.

In both cases, the configuration settings that you have access to are the same. They are described in the following sections.

Displaying the provisioning pages

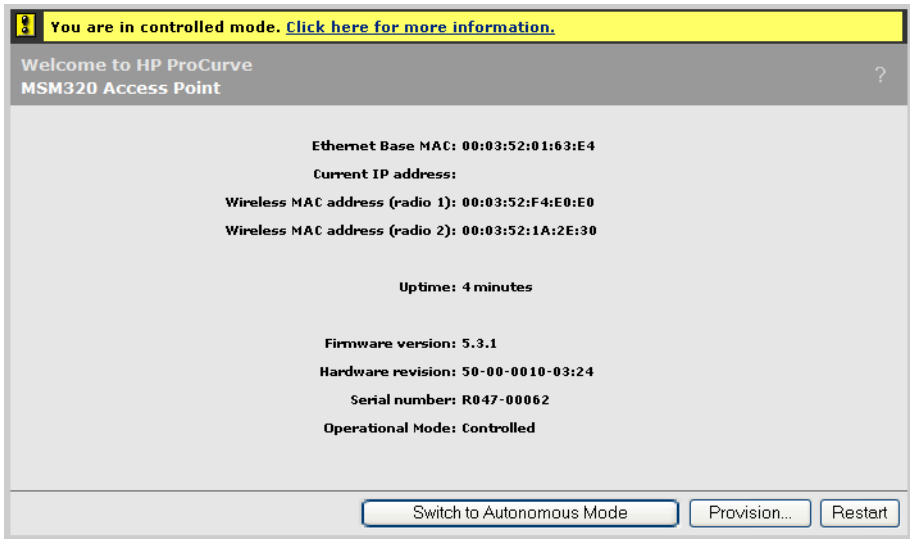
To display the provisioning pages, do the following:

On a service controller

1. Select one of the following in the Network tree:
   - Controlled APs
   - A group
   - An AP
2. In the right pane, select **Provisioning > Connectivity**.
3. Configure provisioning settings as described in the sections that follow.

On an AP in its factory-default state

1. Log in to its management tool.
2. Select **Provision** at the bottom of the home page.



Note

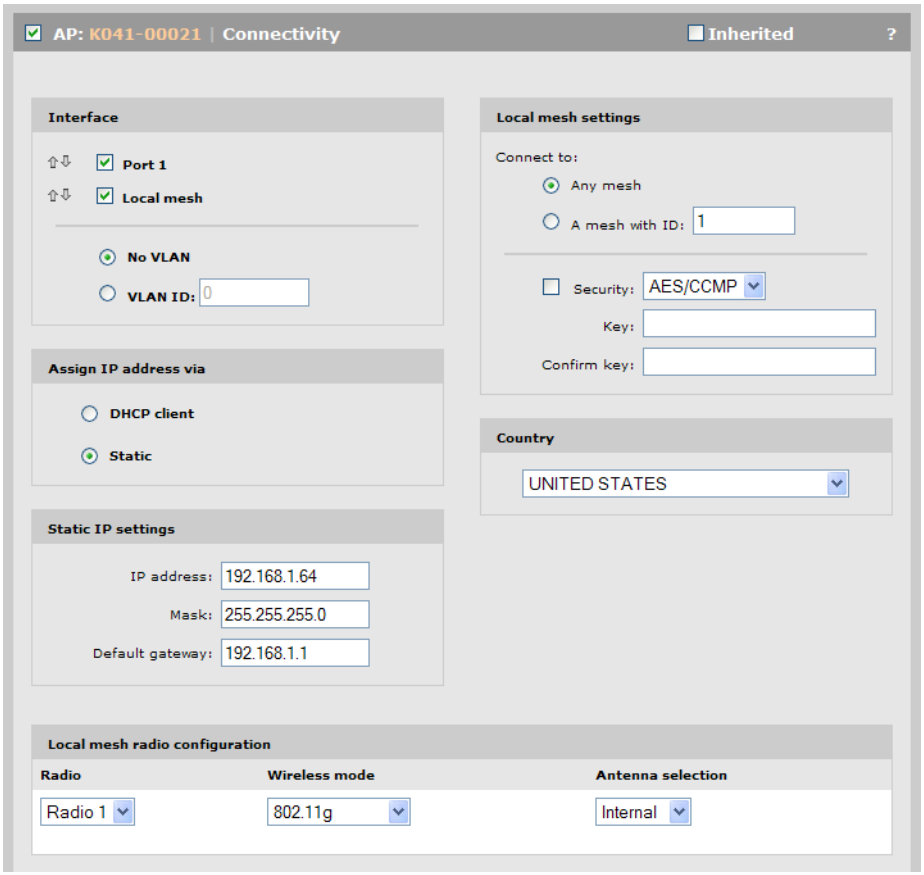
The **Provision** button is only available if the AP is in its factory-default state, meaning it has not yet been provisioned and that the AP has never discovered a service controller (since last factory default). To force an AP into its factory-default state, press and hold its reset button until the status lights blink three times.

3. Configure provisioning settings as described in the sections that follow.

Provisioning connectivity

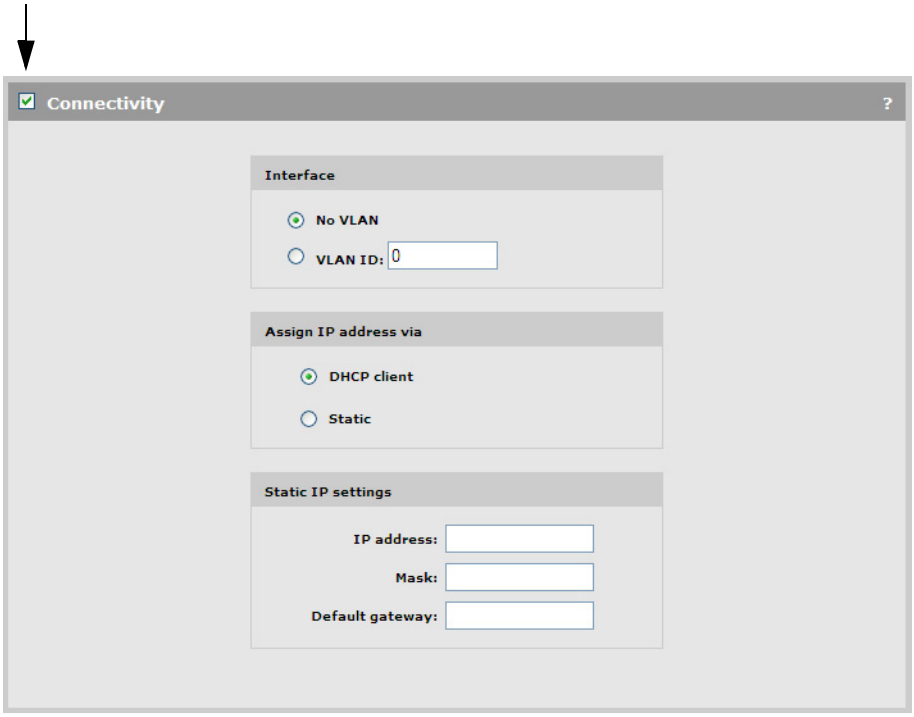
Use the **Provisioning > Connectivity** page to provision connectivity settings for a controlled AP. The following page will appear on all APs except for the MSM317.

Enable provisioning here:



The following page will appear on the MSM317.

Enable provisioning here:



Interface

Select the interface you want to configure and then define its settings using the other options on this page. Set **VLAN ID** if applicable.

Assign IP address via

- **DHCP client:** Address is assigned using a DHCP server. Enable this option to have the interface act as a DHCP client. The AP sends DHCP requests on the specified VLAN. If no VLAN is specified, the request is sent untagged.
- **Static:** Select this option to manually assign an IP address to the interface.

Static IP settings

When you select **Static** for **Assign IP address via**, configure settings in this box.

- **IP address:** Specify the IP address you want to assign to the interface.
- **Address mask:** Specify the appropriate subnet mask for the IP address you specified.
- **Default gateway:** Specify the IP address of the default gateway.

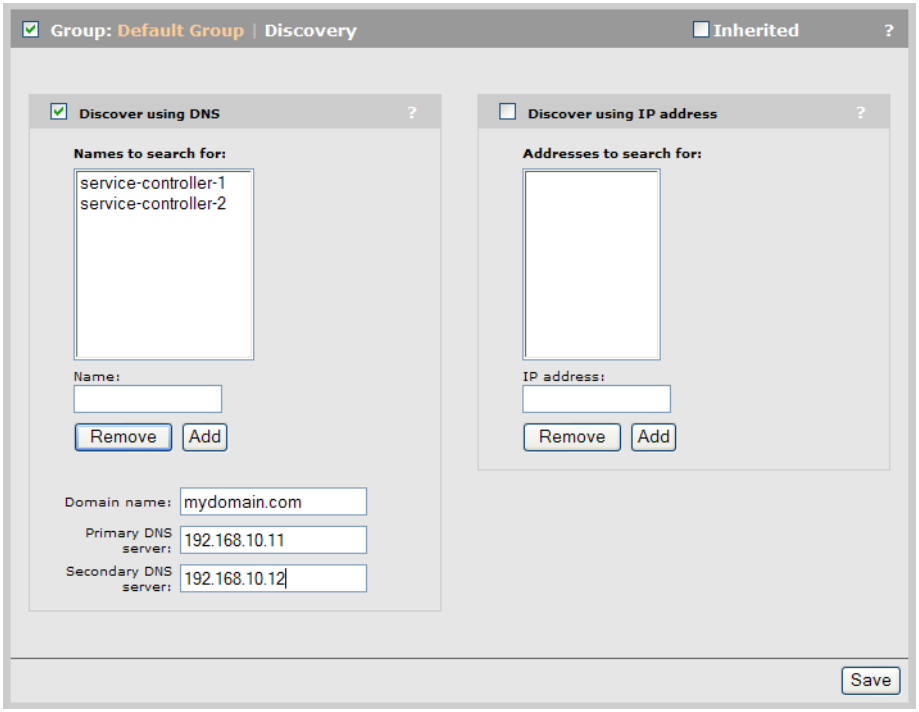
Local mesh settings

For information on provisioning these settings, see *Local mesh on page 13-1*.

Provisioning discovery

Use the **Provisioning > Discovery** page to provision the method a controlled AP uses to discover a service controller. Two options can be provisioned: DNS discovery or discovery via IP address. The following page shows Discovery using DNS provisioned.

Enable provisioning here:



Discover using DNS

The AP attempts to connect with a service controller using the names in the order that they appear in this list.

To discover the service controller on the network, the AP appends each name with the specified **Domain name**.

In the above example, the AP will search for service controllers with the names:

- service-controller-1.mydomain.com
- service-controller-2.mydomain.com

If you define a name that contains a dot, then the domain name is not appended . For example, if the name is **controller.yourdomain.com**, no domain name is appended.

If the AP is operating as a DHCP client, the DHCP server will generally return a domain name when it assigns an IP address to the AP. If you leave the **Domain name** field on this page blank, then the DHCP domain name is appended to the specified names instead.

Discover using IP address

The AP attempts to connect with a service controller using the IP addresses in the order that they appear in this list.

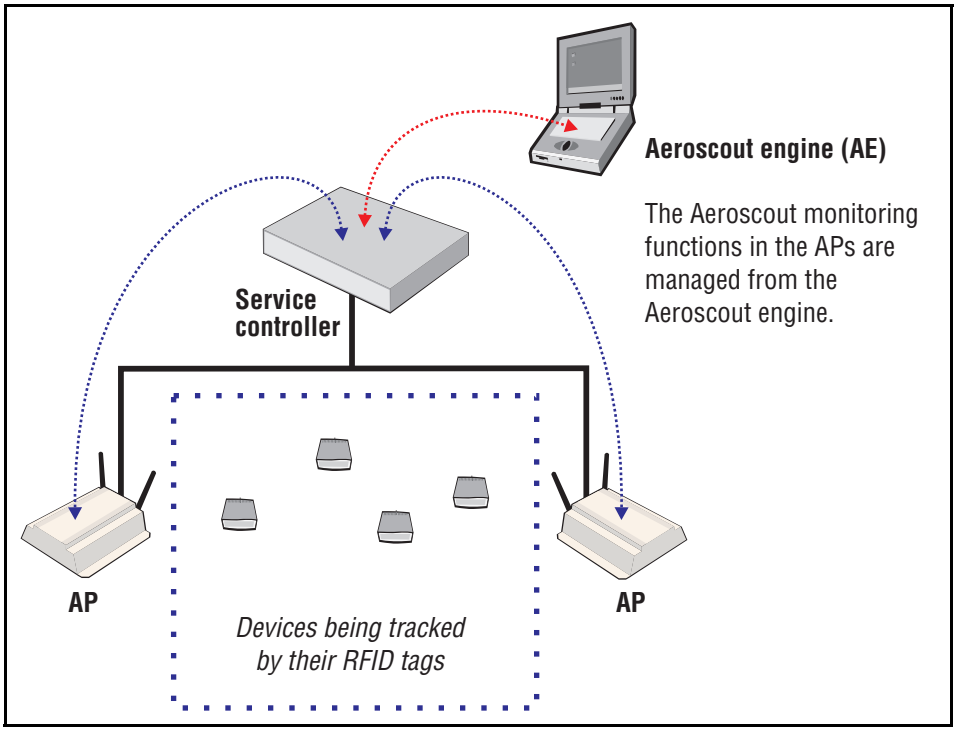
Provisioning summary

The following table defines the potential outcome for all provisioning scenarios.

Connectivity provisioned	Discovery provisioned	Result
No	No	Default behavior is used for connectivity and discovery. See *Discovery of controlled APs on page 3-7*.
No	Yes	Discovery occurs using the provisioned methods on the following interfaces: ■ Last interface on which a service controller was discovered. (Only applies to APs that have previously discovered a service controller.) ■ Untagged on port 1 (Uplink port on the MSM317). ■ All detected VLANs (in sequence) on port 1 (Uplink port on the MSM317).
Yes	No	Discovery methods are used according to the provisioned connectivity settings. See *Discovery of controlled APs on page 3-7*. Note: DHCP discovery is not executed if a static IP address is provisioned.
Yes	Yes	Discovery occurs using the provisioned methods over the provisioned connectivity. The provisioned discovery method is retried indefinitely if it fails, however other discovery methods are not attempted.

AeroScout RTLS

MSM APs and MSM service controllers can be used to provide the Wi-Fi infrastructure for an AeroScout Real-Time Location Tracking (RTLS) system. MSM APs, AeroScout Wi-Fi RFID tags, and the AeroScout MobileView software work together for the purpose of wirelessly tracking the location of valuable assets in real time. The service controller forwards AeroScout tag information from controlled APs to a computer running the AeroScout Engine and MobileView software.


Aeroscout engine (AE)
The Aeroscout monitoring functions in the APs are managed from the Aeroscout engine.
Service controller
AP
AP
Devices being tracked by their RFID tags

Note

- HP ProCurve Networking does not sell or promote AeroScout products. Contact AeroScout for information on obtaining its MobileView software, Wi-Fi RFID tags, and associated hardware. Consult the AeroScout documentation for deployment information.
- To work with MSM APs, the Wi-Fi RFID tags must be configured to send data in the WDS format (4 addresses). Channel allocation on the AP and tag must match as well.

To enable AeroScout support

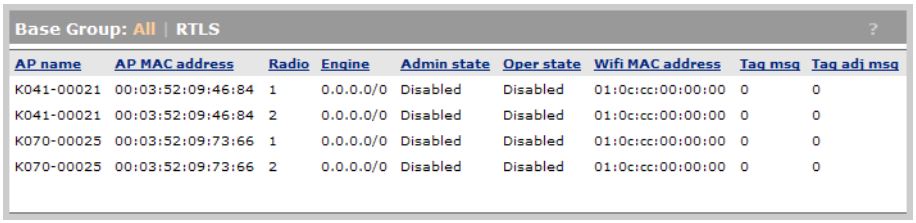
AeroScout support is only available for controlled APs, with radios configured as **Access point only** or **Access point and Local mesh**, and operating in the 2.4 GHz band.

To configure the service controller (and all its controlled APs) to work with AeroScout:

1. Select **Service Controller >> Controlled APs > RTLS.**
2. Select **Enable support for AeroScout tags**.
3. Select **Save**.

Viewing status information

Basic AP and AeroScout tag status information is available by selecting **Service Controller > Controlled APs >> Overview > RTLS**. For example:



Base Group: All | RTLS

AP name	AP MAC address	Radio	Engine	Admin state	Oper state	Wifi MAC address	Tag msg	Tag adj msg
K041-00021	00:03:52:09:46:84	1	0.0.0.0/0	Disabled	Disabled	01:0c:cc:00:00:00	0	0
K041-00021	00:03:52:09:46:84	2	0.0.0.0/0	Disabled	Disabled	01:0c:cc:00:00:00	0	0
K070-00025	00:03:52:09:73:66	1	0.0.0.0/0	Disabled	Disabled	01:0c:cc:00:00:00	0	0
K070-00025	00:03:52:09:73:66	2	0.0.0.0/0	Disabled	Disabled	01:0c:cc:00:00:00	0	0

All AeroScout management and monitoring is performed in the AeroScout software itself. Aeroscout documentation and AeroScout software must be used to operate and monitor the tags.

Software retrieval/update

Software management of controlled APs is automatically performed by the service controller after the AP is discovered (see *Key controlled-mode events on page 3-5*).

If the software version on the AP does not match the version installed on the service controller, new software is installed on the AP by the service controller.

For information on how to update the service controller software see *Software updates on page 15-5*.

Monitoring

The service controller provides a series of pages that present monitoring and status information for controlled APs. You can view these pages for all controlled APs, for all APs in a group, or for just a specific AP. All options appear on the **Overview** menu, which can be reached by selecting:

- **Controlled APs >> Overview**.
- **Controlled APs > [Group name] >> Overview**.
- **Controlled APs > [Group name] > [AP name] >> Overview**.

See the online help for details about the information provided on these status pages.

4

Management

Contents

Management tool 4-2
- Management scenarios 4-2
- Management station 4-2
- Starting the management tool 4-2
- Customizing management tool settings 4-3
- Security policies 4-6
- Security 4-6
- Web server 4-7
- Auto-refresh 4-7

Device discovery 4-8
- Mobility controller discovery 4-8
- Controlled AP discovery 4-9

SNMP 4-10
- Configuring the SNMP agent 4-10

SOAP 4-13
- Configuring the SOAP server 4-13

CLI 4-15
- Configuring CLI support 4-15

System time 4-16

Country 4-17

Management tool

The management tool is a Web-based interface to the service controller that provides easy access to all configuration and monitoring functions.

Management scenarios

For complete flexibility, you can manage the service controller both locally and remotely. The following management scenarios are supported:

- Local management using a computer that is connected to the LAN or Internet port on the service controller. This may be a direct connection or through a switch.
- Remote management via the Internet with or without a VPN connection. See *Securing service controller communications to remote VPN servers on page 12-7* for more information on using the service controller integrated VPN clients to create secure remote connections.

Management station

The *management station* refers to the computer that a manager or operator uses to connect to the management tool. To act as a management station, a computer must:

- Have at least Microsoft Internet Explorer 7.0 or Mozilla Firefox 2.0 installed.
- Be able to establish an IP connection with the service controller.

Note

Before installation, ensure that TCP/IP is installed and configured on the management station. IP addressing can be either static or DHCP. A unique feature of the service controller is its ability to support connections from users that have a preconfigured static IP address.

Starting the management tool

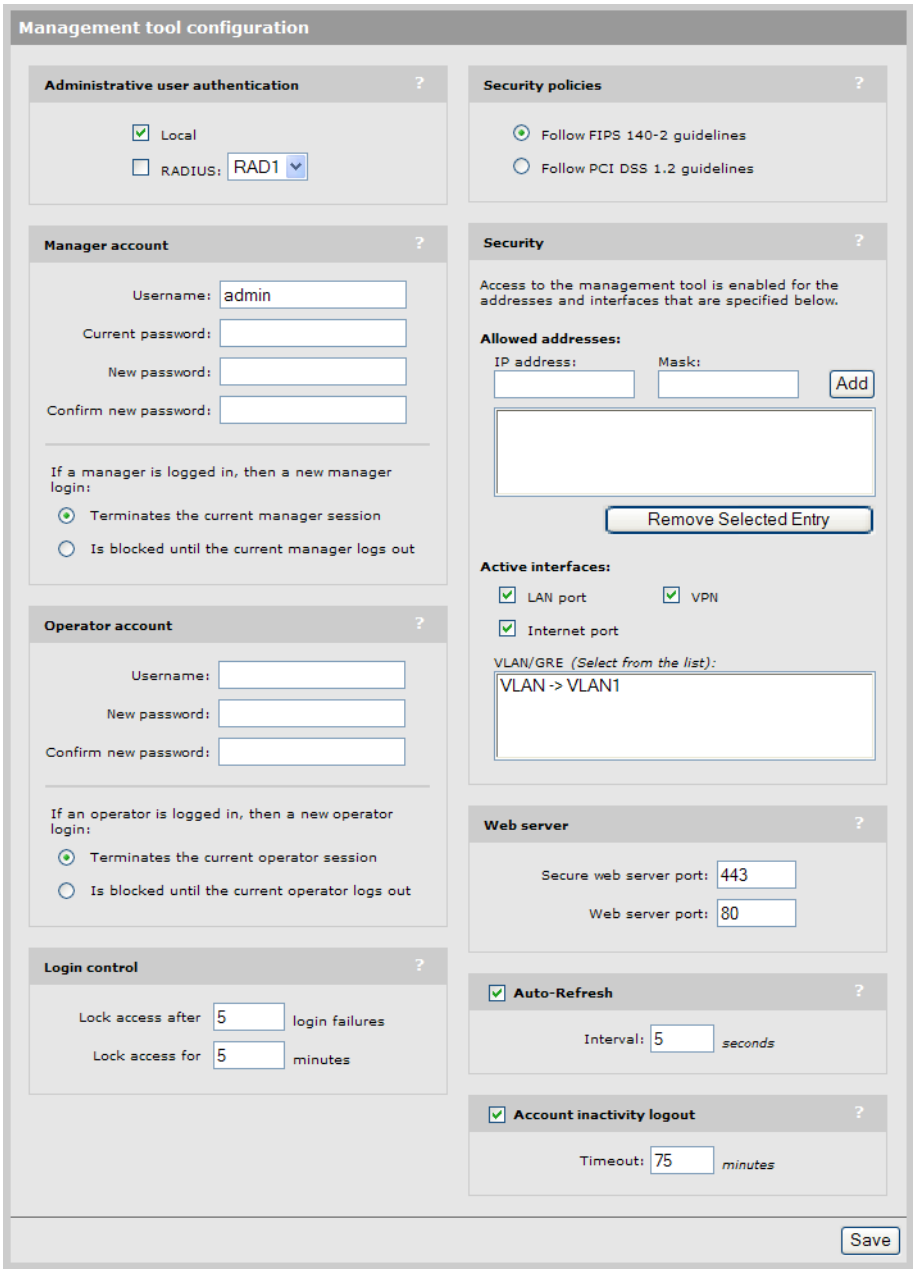
To launch the management tool, specify the following in the address bar of your browser:

`https://Service_Controller_IP_address`

By default, the address 192.168.1.1 is assigned to the LAN port. For information on starting the management tool for the first time, see the relevant guide as described in *Getting started on page 1-10*.

Customizing management tool settings

To customize management tool settings, select **Service Controller >> Management > Management tool**.



Administrative user authentication

Login credentials for administrative users can be verified using local account settings and/or an external RADIUS sever.

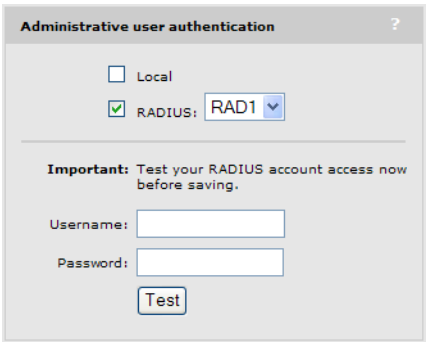
- **Local account settings:** A single manager and operator account can be configured locally under **Manager account** and **Operator account** on this page.
- **RADIUS server:** Using a RADIUS server enables you to have multiple accounts, each with a unique login name and password. Identify manager accounts using the vendor specific attribute **web-administrative-role**. Valid values for this attribute are **Manager** and **Operator**. For attribute information, see *Administrator attributes on page 9-27*. To use a RADIUS server, you must define a RADIUS profile on the **Service Controller >> Authentication > RADIUS profiles** page.

If both options are enabled, the RADIUS server is always checked first. If login is refused by the local account, then the RADIUS server checked.

Authenticating administrative credentials using an external RADIUS server

Configure RADIUS authentication as follows:

1. Define an account for the administrator on the RADIUS server. See *Administrator attributes on page 9-27*.
2. On the service controller, create a RADIUS profile that will connect the service controller to the RADIUS server. See *Configuring a RADIUS server profile on the service controller on page 6-5*.
3. Under **Administrator authentication**, set **Authenticate via** to the RADIUS profile you created. In this example, the profile is called **Rad1**.



4. Test the RADIUS account to make sure it is working before you save your changes. Specify the appropriate username and password and click **Test**.

   (As a backup measure you can choose to enable **Local.** This will allow you to log in using the local account if the connection to the RADIUS server is unavailable.)

Manager and Operator accounts

Two types of administrative accounts are defined: manager and operator.

- The manager account provides full management tool rights.
- The operator account provides read-only rights plus the ability to disconnect wireless clients and perform troubleshooting.

Only one administrator can be logged in at any given time. Options are provided to control what happens when an administrator attempts to log in while another administrator (or the same administrator in a different session) in already logged in. In every case, the manager's rights supersede those of an operator.

The following options can be used to prevent the management tool from being locked by an idle manager or operator:

- **Terminates the current manager session:** When enabled, an active manager or operator session will be terminated by the login of another manager. This prevents the management tool from being locked by an idle session until the **Account inactivity logout** timeout expires.
- **Is blocked until the current manager logs out:** When enabled, access to the management tool is blocked until an existing manager logs out or is automatically logged out due to an idle session.

  An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in.
- **Terminates the current operator session:** When enabled, an active operator's session will be terminated by the login of another operator. This prevents the management tool from being locked by an idle session until the **Account inactivity logout** timeout expires.

  Operator access to the management tool is blocked if a manager is logged in. An active manager session cannot be terminated by the login of an operator.

  An operator session is always terminated if a manager logs in. An active operator session cannot block a manager from logging in.
- **Login control:** If login to the management tool fails five times in a row (bad username and/or password), login privileges are blocked for five minutes. Once five minutes expires, login privileges are once again enabled. However, if the next login attempt fails, privileges are again suspended for five minutes. This cycle continues until a valid login occurs. You can configure the number of failures and the timeout.
- **Account inactivity logout:** By default, if a connection to the management tool remains idle for more than ten minutes, the service controller automatically terminates the session. You can configure the timeout.

Caution

If you forget the manager password, the only way to access the **management tool** is to reset the service controller to factory default settings. See *Appendix C: Resetting to factory defaults*.

Security policies

The default security policy is the US Government **FIPS-140-2 guidelines** (Federal Information Processing Standard); however, **PCI DSS 1.2 guidelines** (Payment Card Industry Data Security Standard) are also supported. The selected security policy affects the login rules in the following ways:

FIPS-140-2 guidelines
The only part of the FIPS-140-2 guidelines that is supported is:

- Passwords must be at least six characters long.
- Passwords must contain at least four different characters.

PCI DSS 1.2 guidelines

- Passwords must be a minimum of seven characters.
- Passwords must contain both numeric and alphabetic characters.
- Users must be locked out after not more than six failed attempts.
- The lockout duration must be at least thirty minutes or until a manager enables the user ID.
- A user must log in again If a session has been idle for more than 15 minutes.

Security

The management tool is protected by the following security features:

- **Allowed IP address:** You can configure a list of subnets from which access to the management tool is permitted.
- **Active interfaces:** You can enable or disable access to the management tool for each of the following:
  - LAN port
  - Internet port
  - VPN
  - VLAN/GRE.

  These settings also apply when SSH is used to access the command line interface.

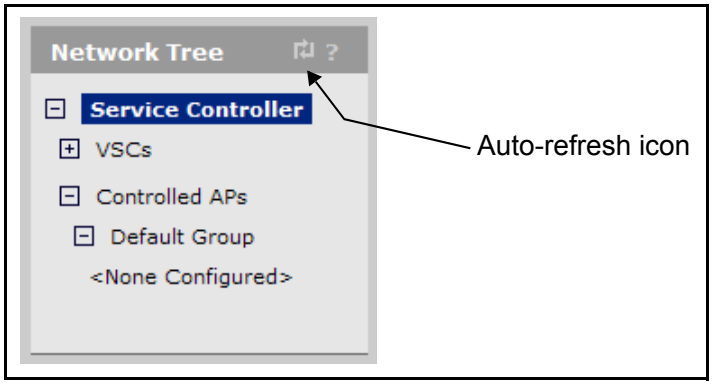
Web server

You can also configure the Web server ports from which access to the management tool is permitted.

- **Secure web server port**: Specify a port number for the service controller to use to provide secure HTTPS access to the management tool**.** Default is 443. Before reaching the management tool login page**,** you must accept a security certificate. The default certificate provided with the service controller will trigger a warning message on most browsers because it is self-signed. To remove this warning message, you must replace the default certificate. See *About certificate warnings on page 5-11*.
- **Web server port**: Specify a port number for the service controller to use to provide standard HTTP access to the management tool**.** These connections are met with a warning, and the browser is redirected to the secure Web server port. Default is 80.

Auto-refresh

This option controls how often the service controller updates the information in group boxes that show the auto-refresh icon in their title bar. Under **Interval,** specify the number of seconds between refreshes.

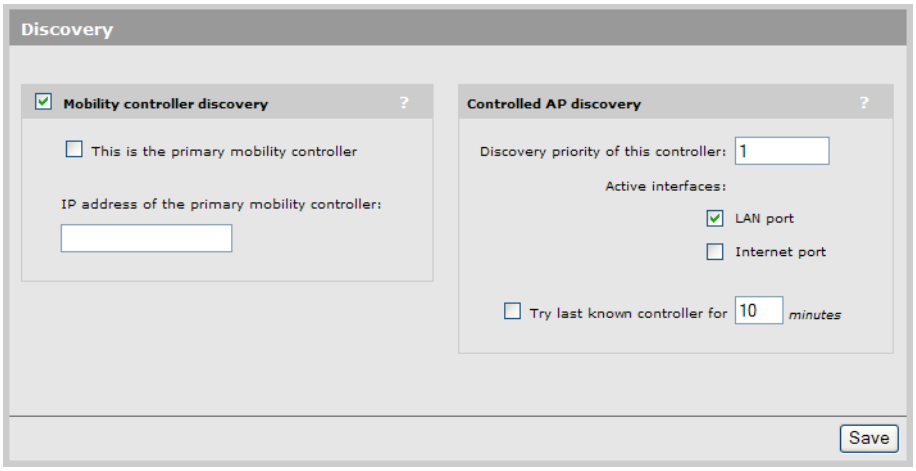


Device discovery

Use this page to define discovery options for:

- Inter-service controller discovery when using the mobility feature
- Service controller discovery by controlled APs

Select **Management > Device discovery** to open the **Discovery configuration** page.



Mobility controller discovery

Enable this option to either define this service controller as the primary mobility controller, or to have it connect to another service controller that is designated as the primary. For more information see *Wireless mobility on page 11-1*.

This is the primary mobility controller

Enable this option to designate this service controller as the primary mobility controller. The primary controller is responsible for the coordination and discovery of all service controllers in the mobile domain.

If you want service controllers to communicate with one another, then you must designate one service controller as the primary. On all other service controllers, disable this option and under **IP address of primary controller**, specify the IP address of the primary service controller.

By default, every service controller is configured to act as the primary mobility controller.

IP address of primary mobility controller

Enter the IP address of the primary mobility controller.

Controlled AP discovery

Discovery priority of this controller

Sets the priority for this service controller when discovered by a controlled AP. A value of 1 indicates the highest priority. A value of 16 indicates the lowest priority.

If multiple service controllers are discovered by a controlled AP, the AP will establish a control channel with the service controller that has the highest priority setting first. If that service controller is already managing the maximum number of controlled APs, the AP will choose the service controller with the next highest priority.

Active interfaces

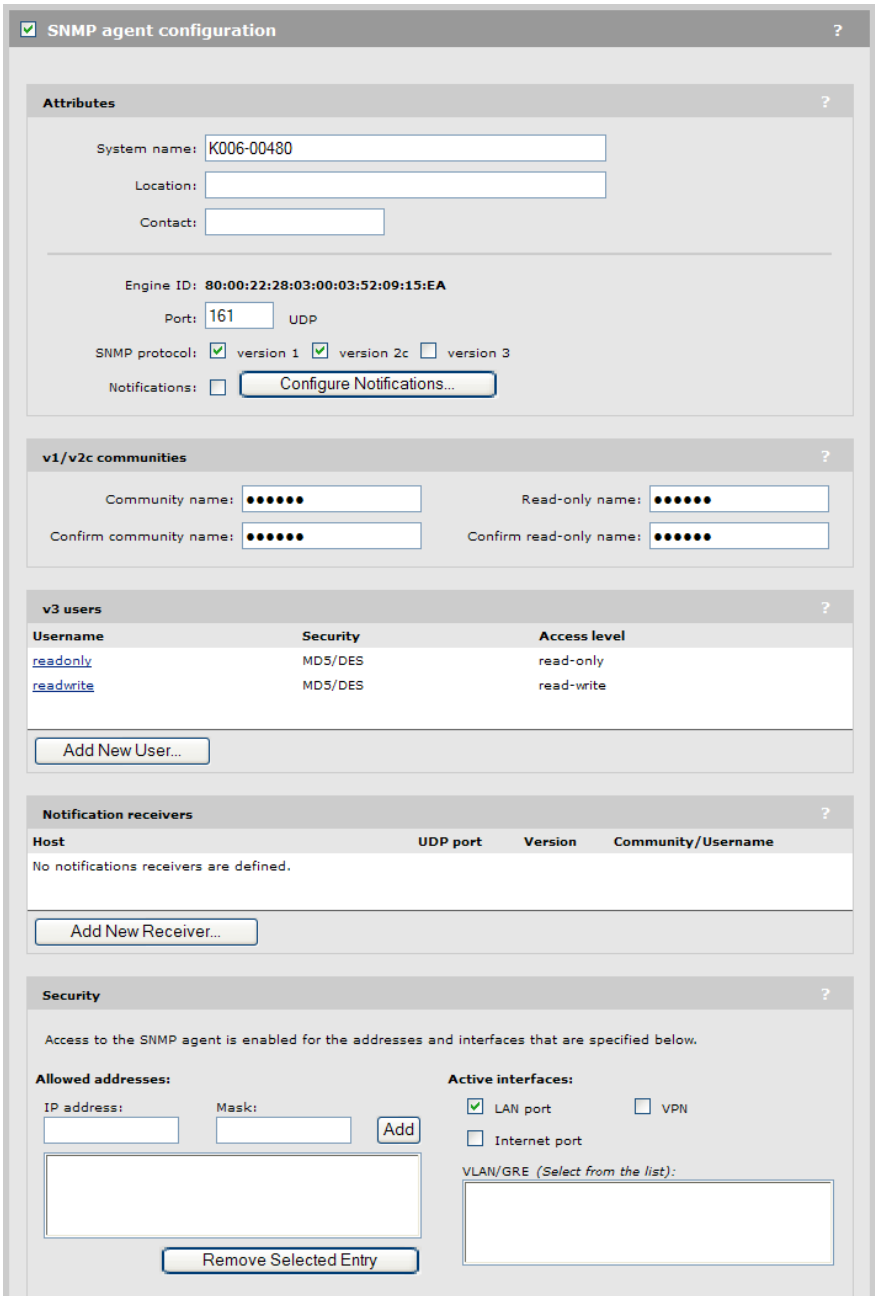
Select the physical interfaces on which the service controller will listen for discovery requests from controlled APs. The control channel to an AP is always established on the interface on which it is discovered.

SNMP

The service controller provides a robust SNMP implementation supporting both industry-standard and custom MIBs. For information on supported MIBs, see the *MSM SNMP MIB Reference Guide*.

Configuring the SNMP agent

Select **Management > SNMP** to open the **SNMP agent configuration** page. By default, the SNMP agent is enabled (**SNMP agent configuration** in title bar is checked). If you disable the agent, the service controller will not respond to SNMP requests.



Attributes

System name
Specify a name to identify the service controller. By default, this is set to the serial number of the service controller.

Location
Specify a descriptive name for the location where the service controller is installed.

Contact
Contact information for the service controller.

Port
Specify the UDP port and protocol the service controller uses to respond to SNMP requests. Default port is 161.

SNMP protocol
Select the SNMP versions that the service controller will support. Default is **Version 1** and **Version 2c**.

Notifications
Select the SNMP versions that the AP will support. Default is **Version 1** and **Version 2c**.

Notifications
When this feature is enabled, the service controller sends notifications to the hosts that appear in the **Notifications receivers** list.

The service controller supports the following MIB II notifications:

- coldStart
- linkUp
- linkDown
- authenticationFailure

In addition, the service controller supports a number of custom notifications. Select **Configure Notifications**. For a descriptions of these notifications, see the online help.

v1/v2 communities

Community name
Specify the password, also known as the read/write name, that controls read/write access to the SNMP agent. A network management program must supply this name when attempting to set or get SNMP information from the service controller. By default, this is set to **private**.

Read-only name
This is the password that controls read-only access to the SNMP agent. A network management program must supply this name when attempting to get SNMP information from the service controller. By default, this is set to **public**.

v3 users

This table lists all defined SNMP v3 users. To add a new user, click **Add New User**. Up to five users are supported. To edit a user, click its link in the **Username** column.

Username
The SNMP v3 username.

Security
Security protocol defined for the user. Authentication type and encryption type are separated a slash. For example, **MD5/DES** indicates **MD5** authentication and **DES** encryption.

Access level
Type of access assigned to the user:

- **Read-only:** The user has read and notify access to all MIB objects.
- **Read-write:** The user has read, write, and notify access to all MIB objects.

Notification receivers

This table lists all defined SNMP notification receivers. SNMP notifications are sent to all receivers in this list. To add a new receiver, click **Add New Receiver**. Up to five receivers are supported. To edit a receiver, click its link in the **Host** column.

Host
The domain name or IP address of the SNMP notifications receiver to which the service controller will send notifications.

UDP port
The port on which the service controller will send notifications.

Version
The SNMP version (1, 2c, 3) for which this receiver is configured.

Community/Username

- For SNMP v1 and v2c, the SNMP Community name of the receiver.
- For SNMP v3, the SNMP v3 Username of the receiver.

Security

Use these settings to control access to the SNMP interface.

- **Allowed addresses**: List of IP address from which access to the SNMP interface is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add.**
- When the list is empty, access is permitted from any IP address.
- **Active interfaces**: Enable the checkboxes that correspond to the interfaces from which to allow access to the SNMP agent. For VLAN, GRE, or Mesh, select from the list. Use Ctrl-click to select multiple objects.

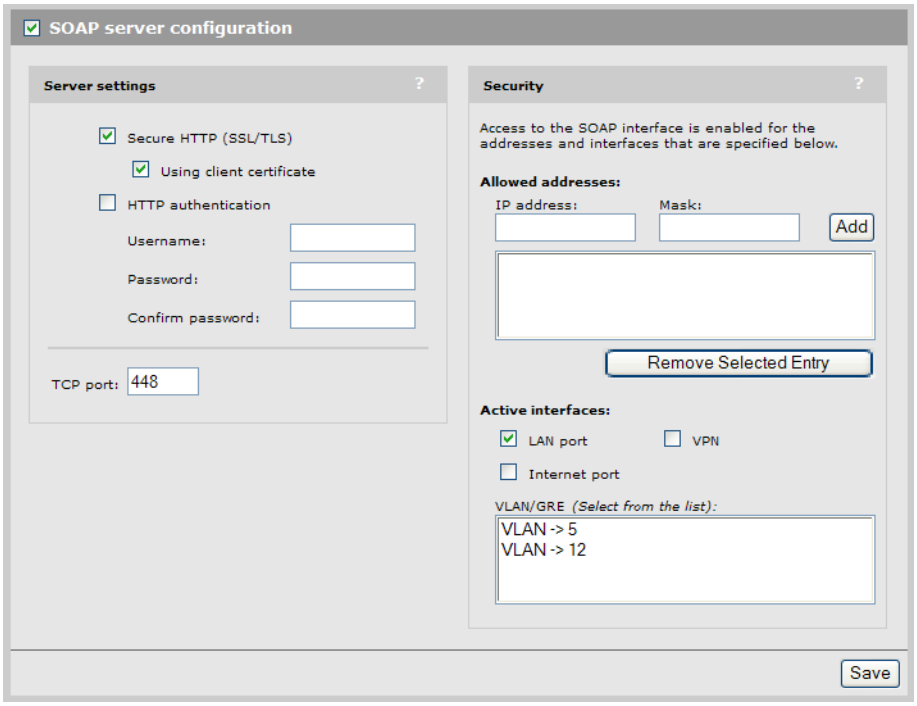
SOAP

The service controller provides a SOAP interface that can be used by SOAP-compliant client applications to perform configuration and management tasks.

The SOAP/XML SDK is available on the HP ProCurve Networking manuals page at: **www.procurve.com/manuals** under **MSM7xx Controllers**.

Configuring the SOAP server

Select **Management > SOAP** to open the **SOAP server configuration** page. By default, the SOAP server is enabled (**SOAP server configuration** in title bar is checked).



Server settings

Secure HTTP (SSL/TLS)

Enable this option to configure the SOAP server for SSL/TLS mode. When enabled, the Secure Sockets Layer (SSL) protocol must be used to access the SOAP interface.

Using client certificate

When enabled, the use of a X.509 client certificate is mandatory for SOAP clients.

HTTP authentication

When enabled, access to the SOAP interface is available via HTTP with the specified username and password.

TCP port

Specify the number of the TCP port that SOAP uses to communicate with remote applications. Default is 448.

Security

Use these settings to control access to the SOAP interface.

- **Allowed addresses**: List of IP address from which access to the SOAP interface is permitted. To add an entry, specify the **IP address** and appropriate **Mask**, and then select **Add.**

  When the list is empty, access is permitted from any IP address.

- **Active interfaces**: Enable the checkboxes that correspond to the interfaces from which to allow access to the SOAP interface.

Security considerations

- The SOAP server is configured for SSL/TLS mode, and the use of a X.509 client certificate is mandatory for SOAP clients.
- The SOAP server is configured to trust all client certificates signed by the default SOAP CA installed on the service controller.
- Users should generate and install their own SOAP CA private key/public key certificate to protect their devices from unauthorized access. This is important because the default SOAP CA and a valid client certificate are provided as an example to all customers. (See *Managing certificates on page 5-6*.)

CLI

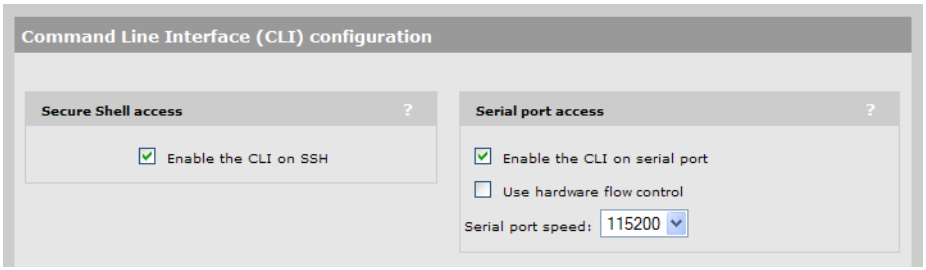
The service controller provides a command line interface that can be used to perform configuration and management tasks via the serial port or an IP connection on any of the service controller interfaces, including the LAN port, Internet port, or VPN/GRE tunnel.

For information on using the CLI, see the *CLI Reference Guide*.

A maximum of three concurrent CLI sessions are supported regardless of the connection type.

Configuring CLI support

Select **Management > CLI** to open the **Command Line Interface (CLI) configuration** page.



Secure shell access

Enable this option to allow access to the CLI via an SSH session. The CLI supports SSH on the standard TCP port (22).

Connectivity and login credentials for SSH connections use the same settings as defined for management tool on the **Service controller >> Management > Management tool** page.

- SSH connections to the CLI can be made on any active interface. Support for each interface must be explicitly enabled under **Security.**
- The login credentials for SSH connections are the same as those defined under **Administrative user authentication** and **Manager account**. Operator accounts are not supported.

Note

SSH logins always use the local manager username and password, even if **Administrator authentication** is set to use an external RADIUS server.

The following SSH clients have been tested with the CLI. Others may work as well:

- OpenSSH
- Tectia
- SecureCRT
- Putty.

Serial port access

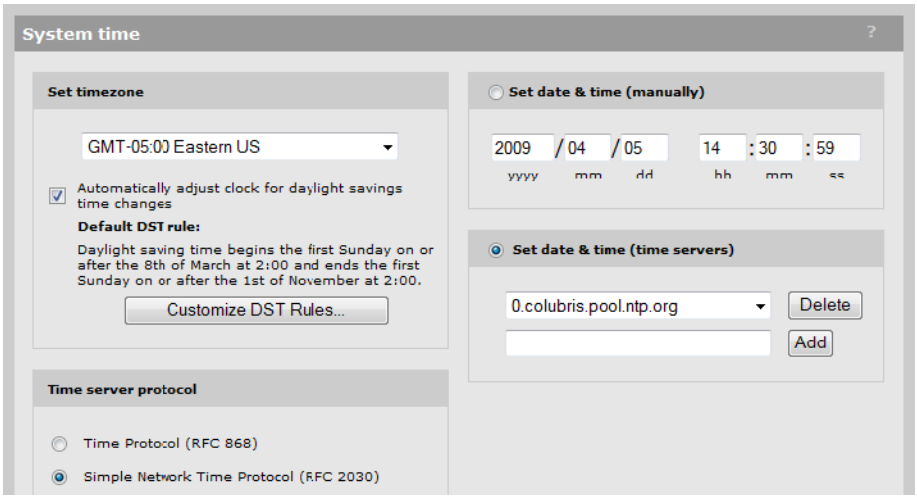
- **Enable the CLI on serial port**: Enable this option to allow access to the CLI through the serial port.
- **Use hardware flow control**: Enable hardware flow control on the serial port connection. Flow control keeps the data flow at an efficient pace. Too much data arriving before a device can handle it causes data overflow, meaning the data is either lost or must be retransmitted.
- **Serial port speed**: Select the speed of your serial port connection.

System time

Select **Management > System time** to open the **System time** page. This page enables you to configure the time server and time zone information.

Note

The system time page on the MSM765zl is a read-only page that displays the current time.


System time
Set timezone
GMT-05:00 Eastern US
Automatically adjust clock for daylight savings time changes
Default DST rule:
Daylight saving time begins the first Sunday on or after the 8th of March at 2:00 and ends the first Sunday on or after the 1st of November at 2:00.
Customize DST Rules...
Time server protocol
Time Protocol (RFC 868)
Simple Network Time Protocol (RFC 2030)
Set date & time (manually)
2009 / 04 / 05
yyyy mm dd
14 : 30 : 59
hh mm ss
Set date & time (time servers)
0.colubris.pool.ntp.org
Delete
Add

Note

Correct time is particularly important when the service controller is managing controlled APs, as the time configured on the service controller is used on all controlled APs. Synchronization and certificate problems can occur if the service controller time is not accurate.

1. Set **timezone** and daylight savings time and as appropriate. Optionally use the Customize DST Rules button to set custom rules.
2. Set **Time server protocol** to **Simple Network Time Protocol** (default setting).
3. Select **Set date & time (time servers)** and then select the desired time server. Time servers can be located on the Internet or LAN ports. **Add** other servers if desired. The service controller contacts the first server in the list. If the server does not reply, the service controller tries the next server and so on. By default, the list contains two ntp vendor zone pools that are reserved for HP ProCurve Networking devices. By using these

pools, you will get better service and keep from overloading the standard ntp.org server. For more information visit: www.pool.ntp.org.

4. Select **Save** and verify that the date and time are updated accurately.

Country

The Country sub-menu is not available on service controllers delivered with a fixed country setting. The country for which the service controller is configured to operate is displayed on the management tool home page.

Select **Management > Country** time to open the **Country** page. This page enables you to configure the country in which the service controller operates.

Caution

Do not change Country to a country other than the one in which the service controller operates. Failing to heed this caution may violate the regulatory compliance of controlled-mode MAPs managed by this service controller.

Note

After changing the country code controlled APs must be synchronized as described in *Synchronizing APs on page 3-22*.

5

Security

Contents

Overview 5-2

Firewall 5-2
- Firewall presets 5-3
- Firewall configuration 5-4
- Customizing the firewall 5-5

Managing certificates 5-6
- Trusted CA certificate store 5-6
- Certificate and private key store 5-9
- Certificate usage 5-10
- About certificate warnings 5-11
- IPSec certificates 5-12

Overview

The service controller provides many configurable security features, including firewall, authentication, and VPN (virtual private network).

This chapter describes how to use the firewall and manage security certificates.

Authentication options, previously on the **Security** menu are now found on the **Authentication** menu. See *Chapter 6: Authentication services*, and *Chapter 7: User authentication*.

VPN options, previously on the **Security** menu are now found on the **VPN** menu. See *Chapter 12: Working with VPNs*.

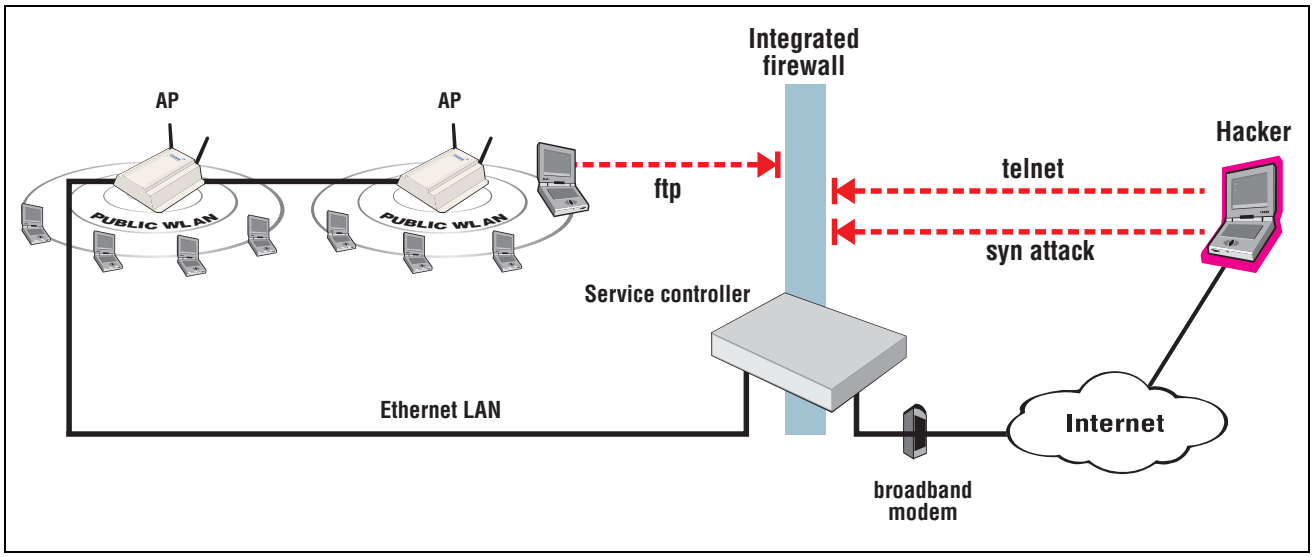
For information on extending WPA termination from the AP to the service controller, see *Terminate WPA at the service controller on page 2-14*.

Firewall

To safeguard your network from intruders, the service controller features a customizable stateful firewall. The firewall operates on the traffic streaming through the Internet port. It can be used to control both incoming and outgoing data.

A number of predefined firewall rules let you achieve the security level you need without going to the trouble of designing your own rules. However, you can create a completely custom set of firewall rules to suit your particular networking requirements, if necessary.

If the service controller is connected to a wired LAN, the firewall protects the wired LAN as well.



Firewall presets

The easiest way to use the firewall is to use one of the preset settings. Two levels of security are provided:

- **High**: Permits all outgoing traffic, except NetBIOS (TCP and UDP). Blocks all externally initiated connections.
- **Low**: Permits all incoming and outgoing traffic, except for NetBIOS traffic. Use this option if you require active FTP sessions.

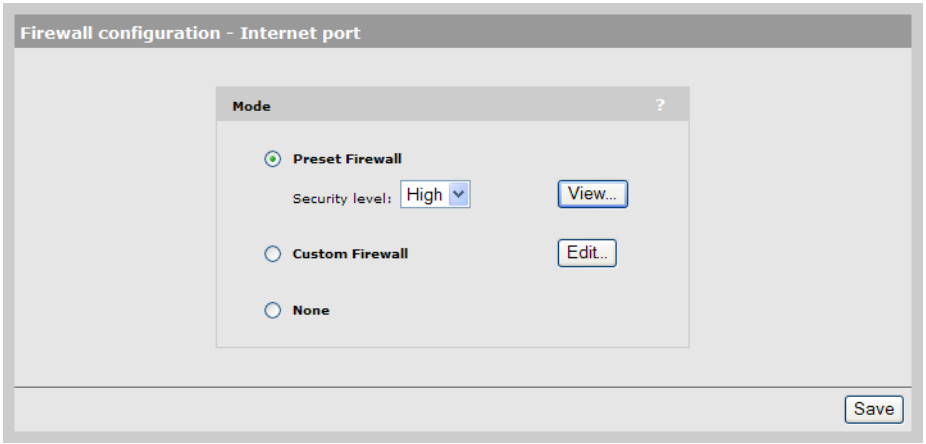
The following tables indicate how some common applications are affected by the preset firewall settings.

Outgoing traffic	**Firewall setting**	
Application	**Low**	**High**
FTP (passive mode)	Passed	
FTP (active mode)	Passed	
Web (HTTP, HTTPS)	Passed	
SNMP	Passed	
Telnet	Passed	
Windows networking	Blocked	
ping	Passed	
PPTP from client station to remote server	Passed	
NetMeeting (make call)	Passed	
IPSec pass-through	Passed	
NetBIOS	Blocked	

Incoming traffic	Firewall setting	
Application	**Low**	**High**
FTP (passive mode)	Passed	Blocked
FTP (active mode)	Passed	Blocked
Web (HTTPS)	Passed	Blocked
Web (HTTP)	Passed	Blocked
Telnet	Passed	Blocked
Windows networking	Passed	Blocked
PPTP from remote client to a server on the local network	Passed	Blocked
ping client on local network	Passed	Blocked
IPSec pass-through	Passed	Blocked
NetBIOS	Passed	Blocked
NetMeeting (receive call)	Passed	Blocked

Firewall configuration

To configure a firewall, select **Service Controller >> Security > Firewall**. The **Firewall configuration** page opens.

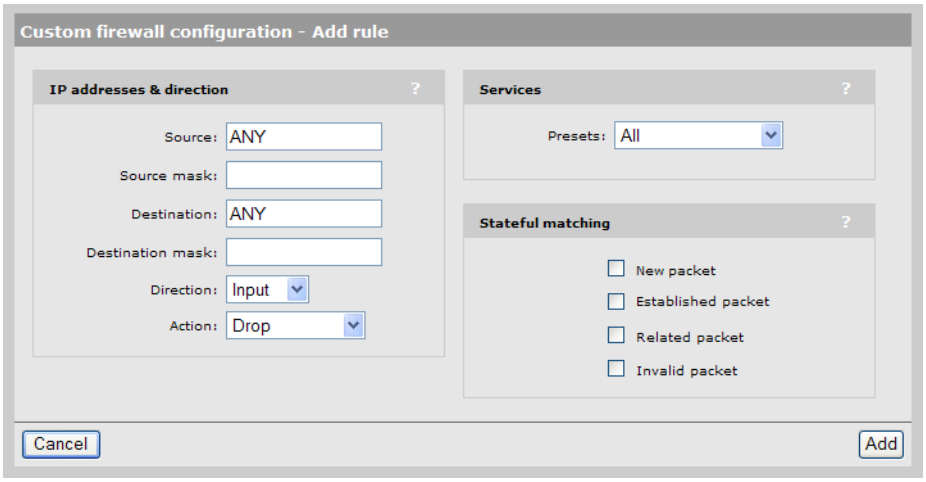


- Select **Preset firewall** to use a preconfigured firewall setting of **High** or **Low.** Select **View** to see the firewall rules for the selected setting.
- Select **Custom firewall** if you have specific security requirements. This setting enables you to target specific protocols or ports.

Customizing the firewall

To customize the firewall, you define one or more rules. A rule lets you target a specific type of data traffic. If the service controller finds data traffic that matches the rule, the rule is triggered, and the traffic is rejected or accepted by the firewall.

To add a rule, select **Custom Firewall** on page **Security > Firewall**, select **Edit**, and then select **Add New Rule**.



Rules operate on IP datagrams (sometimes called *packets)*. Datagrams are the individual packages of data that travel on an IP network. Each datagram contains addressing and control information along with the data it is transporting. The firewall analyses the addressing and control information to apply the rules you define.

The service controller applies the firewall rules in the order that they appear in the list. An intelligent mechanism automatically adds the new rules to the list based on their scope. Rules that target a large amount of data are added at the bottom. Rules that target specific datagram attributes are added at the top.

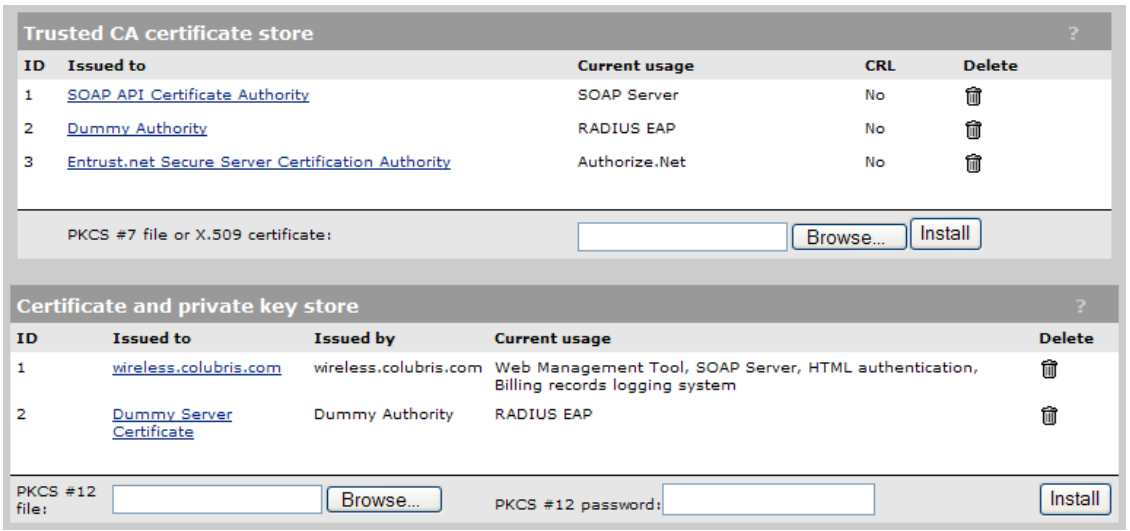
Managing certificates

Digital certificates are electronic documents that are used to validate the end parties or entities involved in data transfer. These certificates are normally associated with X.509 public key certificates and are used to bind a public key to a recognized party for a specific time period.

The service controller uses certificates for the authentication and/or encryption of data exchanged with peers. The following services make use of certificates:

- Managers or operators accessing the service controller management tool
- HTML users accessing the public access interface
- SOAP clients communicating with the service controller SOAP server
- RADIUS EAP-TLS
- RADIUS EAP-PEAP (server certificate only)
- IPSec connections
- NOC authentication (see *NOC authentication on page 9-59*.)

The certificate stores provide a repository for managing all certificates (except for those used by IPSec and NOC authentication). To view the certificate stores, select **Service Controller >> Security > Certificate stores**.



Trusted CA certificate store

This list displays all root CA certificates installed on the service controller. The service controller uses the CA certificates to validate the certificates supplied by peers during authentication. Multiple CA certificates can be installed to support validation of peers with certificates issued by different CAs.

The service controller uses these certificates to validate certificates supplied by:

- Managers or operators accessing the service controller management tool
- HTML users accessing the public access interface
- SOAP clients communicating with the service controller SOAP server
- RADIUS EAP

Items provided in this list are as follows:

ID
A sequentially assigned number to help identify certificates with the same common name.

Issued to
Name of the certificate holder. Select the name to view the contents of the certificate.

Current usage
Lists the services that are currently using this certificate.

CRL
Indicates if a certificate revocation list is bound to the certificate. An X.509 certificate revocation list is a document produced by a certificate authority (CA) that provides a list of serial numbers of certificate that have been signed by the CA but that should be rejected.

Delete
Select to remove the certificate from the certificate store.

Installing a new CA certificate

1. Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.
2. Select **Install** to install a new CA certificate.

CA certificate import formats

The import mechanism supports importing the ASN.1 DER encoded X.509 certificate directly or as part of two other formats:

- PKCS #7 (widely used by Microsoft products)
- PEM, defined by OpenSSL (popular in the Unix world)

- The CRL can be imported as an ASN.1 DER encoded X.509 certificate revocation list directly or as part of a PEM file.

Content and file format	Items carried in the file	Description
ASN.1 DER encoded X.509 certificate	One X.509 certificate	This is the most basic format supported, the certificate without any envelope.
X.509 certificate in PKCS #7 file	One X.509 certificate	Popular format with Microsoft products.
X.509 certificate in PEM file	One or more X.509 certificates	Popular format in the Unix world. X.509 DER certificate is base64 encoded and placed between "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----" lines. Multiple certificates can be repeated in the same file.
ASN.1 DER encoded X.509 CRL	One X.509 CRL	Most basic format supported for CRL.
X.509 CRL in PEM file	One X.509 CRL	Same format as X.509 certificate in PEM format, except that the lines contain BEGIN CRL and END CRL.

Default CA certificates

The following certificates are installed by default:

- **SOAP API Certificate Authority:** Before allowing a SOAP client to connect, the service controller checks the certificate supplied by a SOAP client to ensure that it is issued by a trusted certificate authority (CA).
- **Dummy Authority:** Used by the internal RADIUS server. You should replace this with your own CA certificate.

Note For security reasons, you should replace the default certificates with your own.

Certificate and private key store

This list displays all certificates installed on the service controller. The service controller uses these certificates and private keys to authenticate itself to peers.

Items provided in this list are as follows:

ID
A sequentially assigned number to help identify certificates with the same common name.

Issued to
Name of the certificate holder. Select the name to view the contents of the certificate.

Issued by
Name of the CA that issued the certificate.

Current usage
Lists the services that are currently using this certificate.

Delete
Select to remove the certificate from the certificate store.

Installing a new private key/public key certificate chain pair

Note

RADIUS EAP certificates must have the X.509 extensions. Information about this is available in the Microsoft knowledgebase at:
http://support.microsoft.com/kb/814394/en-us

The certificate you install must:

- Be in PKCS #12 format.
- Contain a private key (a password controls access to the private key).
- Not have a name that is an IP address. The name should be a domain name containing at least one dot. If you try to add a certificate with an invalid name, the default certificate is restored.

The common name in the certificate is automatically assigned as the domain name of the service controller.

1. Specify the name of the certificate file or select **Browse** to choose one from a list. Certificates must be in PKCS #7 format.
2. Specify the **PKCS #12 password**.
3. Select **Install** to install the certificate.

Default installed private key/public key certificate chains

The following private key/public key certificate chains are installed by default:

- **wireless.colubris.com:** Default certificate used by the management tool, SOAP server, and HTML-based authentication.

- **Dummy Server Certificate:** Used by the internal RADIUS server. This certificate is present only to allow EAP-PEAP to work if the client chooses not to verify the server's certificate. You should replace this with your own certificate for maximum security.

Note

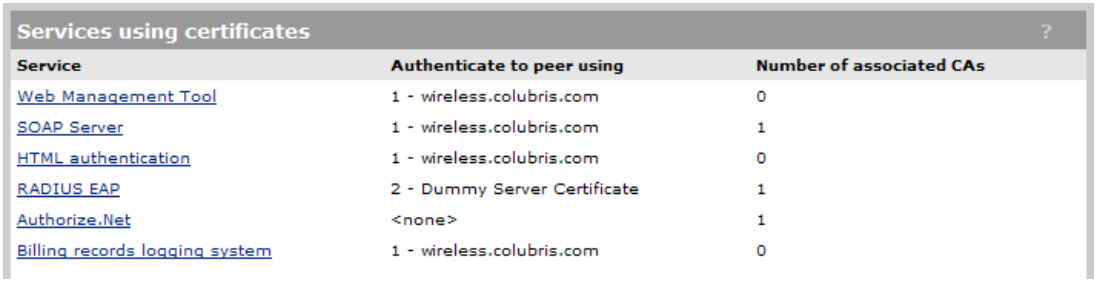
When a Web browser connects to the service controller using SSL, the service controller sends only its own SSL certificate to the browser. This means that if the certificate has been signed by an intermediate certificate authority, and if the Web browser only knows about the root certificate authority that signed the public key certificate of the intermediate certificate authority, the Web browser does not get the whole certificate chain it needs to validate the identity of the service controller. Consequently, the Web browser issues security warnings. To avoid this problem, make sure that you install the entire certificate chain when you install a new certificate on the service controller.

Note

An SNMP notification is sent to let you know when the service controller SSL certificate is about to expire if you enable the **Notifications** option on the **Service Controller >> Management > SNMP** page and then click **Configure Notifications** and enable the **Certificate about to expire** notification under **Maintenance**.

Certificate usage

To see the services that are associated with each certificate, select **Security > Certificate usage**. With the factory default certificates installed, the page will look like this:



Service

Name of the service that is using the certificate. To view detailed information on the certificate select the service name.

Authenticate to peer using

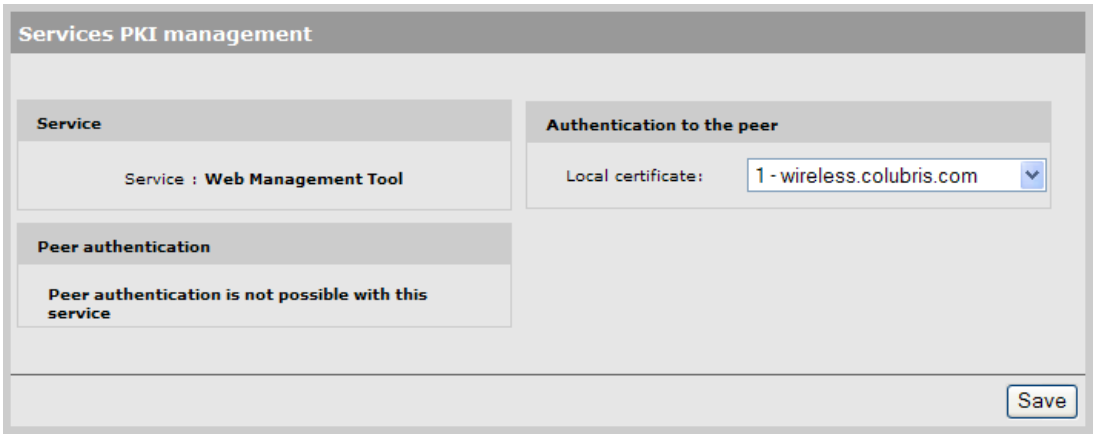
Name of the certificate and private key. The service controller is able to prove that it has the private key corresponding to the public key in the certificate. This is what establishes the service controller as a legitimate user of the certificate.

Number of associated CAs

Number of CA certificates used by the service.

Changing the certificate assigned to a service.

Select the service name to open the Certificate details page. For example, if you select **Web management tool**, you will see:



Under **Authentication to the peer**, select a new **Local certificate** and then select **Save**.

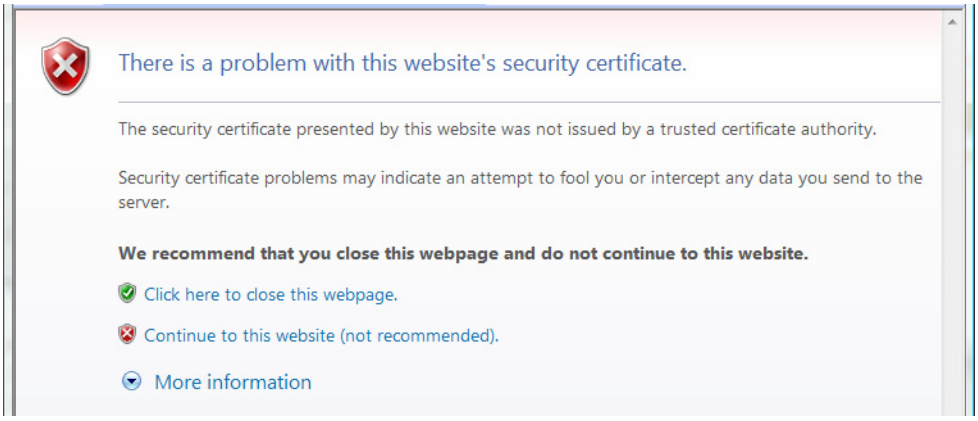
About certificate warnings

Access to the management tool and the public access interface Login page must occur through a secure connection (SSL). Until a valid, trusted certificate is installed on the service controller, certificate warnings will appear at login.

To continue to work with the management tool without installing a certificate, proceed as follows: At the security certificate prompt, in Microsoft Internet Explorer 7, select **Continue to this website**; in Firefox 2, select **Accept this certificate temporarily for this session** and **OK**.

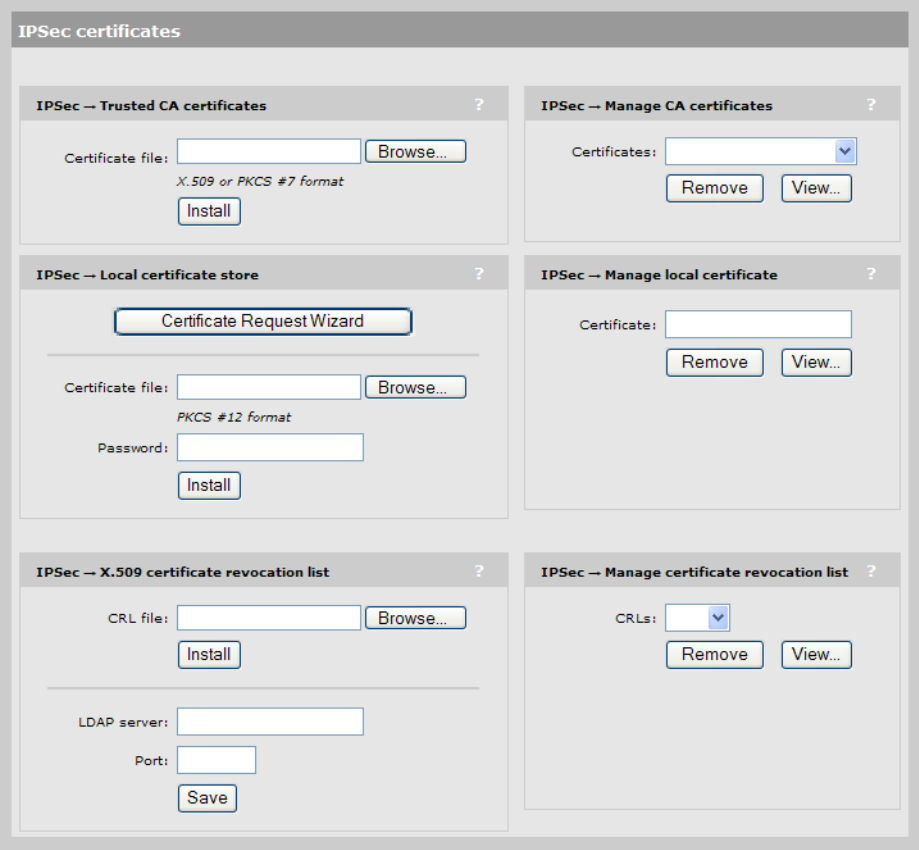
To eliminate these warnings you can purchase a valid SSL certificate (from a source such as Verisign) that will work with the default configuration of your Web browser, and install it on the service controller.

The following is an example of a security warning displayed by Internet Explorer 7.


There is a problem with this website's security certificate.
The security certificate presented by this website was not issued by a trusted certificate authority.
Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
More information

IPSec certificates

IPSec certificates are managed on the lower portion of the **Service Controller >> VPN > IPSec** page.



IPSec — Trusted CA certificates

The service controller uses the CA certificates to validate the certificates supplied by peers during the authentication process. Multiple CA certificates can be installed to support validation of peers with certificates issued by different CAs.

- **Certificate file**: Specify the name of the certificate file or select **Browse** to choose from a list. CA certificates must be in X.509 or PKCS #7 format.
- **Install**: Select to install the specified certificate.

IPSec — Manage CA certificates

Use this box to manage the root CA certificate.

- **Certificate**: Select from a list of installed certificates.
- **Remove**: Delete the item shown under **Certificate.**
- **View:** Open the item shown under **Certificate** for viewing.

IPSec — Local certificate store

This is the certificate that the service controller uses to identify itself to IPSec peers.

Note If the local certificate includes a CA certificate, both certificates are installed.

- **Certificate Request Wizard**: Helps you to generate a certificate request that can be used to obtain a signed certificate from a certificate authority. Once you obtain the certificate, you can use the **Certificate Request Wizard** to install it on the service controller.
- **Certificate file**: Specify the name of the certificate file or select **Browse** to choose from a list.
- **Password**: Specify the certificate password.
- **Install**: Select to install the certificate.

IPSec — Manage local certificate

Use this box to manage the local certificate.

- **Certificate**: Shows the common name of the installed certificate.
- **Remove**: Delete the item shown under **Certificate.**
- **View**: Open the item shown under **Certificate** for viewing.

IPSec — X.509 certificate revocation list

Use this box to update the certificate revocation list (CRL) that is issued by the certificate authority.

The service controller uses the CRL to determine if the certificates provided by clients during the authentication process have been revoked. The service controller will not establish a security association with a client that submits a revoked certificate.

The service controller can obtain a CRL in two ways:

- You can manually install it.
- The service controller can automatically install a CRL based on information contained in a client certificate. This occurs only if a CRL is not installed, or if the installed CRL is expired.
- **CRL file**: Specify the name of the CRL file or select **Browse** to choose from a list.
- **Install**: Select to install the specified CRL.
- **LDAP server**: A client certificate may contain a list of locations where the CRL can automatically be retrieved. This location may be specified as an HTTP URL, FTP URL, LDAP URL, or LDAP directory. If the LDAP URL or directory is incomplete, the service controller uses the location you specify to resolve the request. Incomplete HTTP or FTP URLs fail.
- **Port**: Port on the LDAP server. Default is 389.

IPSec — Manage certificate revocation list

Use this box to manage the CRL.

- **CRLs**: Shows a list of installed certificate revocation lists.
- **Remove**: Deletes the item shown under **CRLs.**
- **View**: Opens the item shown under **CRLs** for viewing.

6

Authentication services

Contents

Overview 6-2

Using the integrated RADIUS server 6-2
- Server configuration 6-3
- User account configuration 6-4

Using a third-party RADIUS server 6-5
- Configuring a RADIUS server profile on the service controller 6-5

Using an Active Directory server 6-9
- Active Directory configuration 6-9
- Configuring an Active Directory group 6-12
- Configuring a VSC to use Active Directory 6-14

Configuring global 802.1X settings 6-15

Configuring MAC lists 6-15

Overview

Before you can perform key authentication tasks such as setting up user authentication, you need to first configure the desired authentication services related to the internal RADIUS server or external RADIUS servers or Active Directories.

Once these services are configured, see *Chapter 7: User authentication*.

Using the integrated RADIUS server

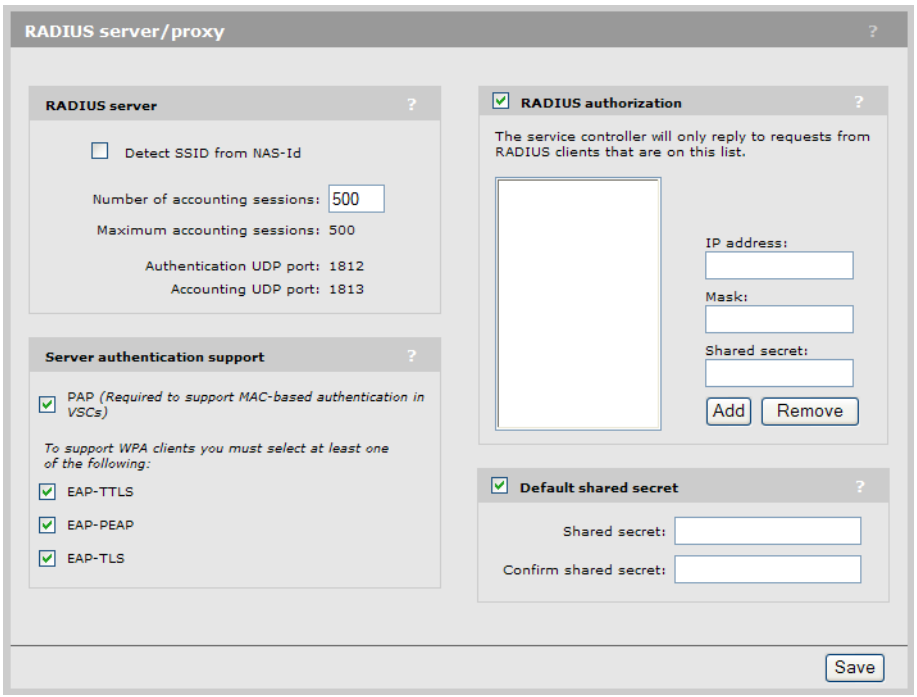
The internal RADIUS server is not intended as a replacement for the high-end/high-performance RADIUS server required for large scale deployments. Rather, it is offered as a cost-effective solution for managing small hotspots or enterprise networks.

Primary features

- Provides termination of 802.1X sessions at the service controller for clients using WPA/WPA2 with EAP-PEAP, EAP-TLS and EAP-TTLS. Support for other EAP protocols is viable using proxy mode.
- Provides MAC-based authentication of wireless users connected to both controlled and autonomous APs.
- Can be used to validate login credentials for HTML-based users.
- All locally defined user account options (user accounts, account profiles, and subscription plans) presented on the **Service Controller >> Users** menu are handled by the internal RADIUS server.
- Allows RADIUS accounting data to be sent to an external RADIUS server. (The internal RADIUS server does not provide support for accounting.)
- Local user accounts and account profiles have been designed to match the same functionality and support as can be provided by an external RADIUS server. Most of the AVPairs supported on an external RADIUS server are also supported by the integrated RADIUS server.

Server configuration

Configuration of the integrated RADIUS server is done using the **Service Controller >> Authentication > RADIUS server** page. In most cases, the default settings on this page will not need to be changed.



Configuration parameters

RADIUS server

Detect SSID from NAS-Id

Enable this option when working with third-party APs to permit the service controller to retrieve the SSID assigned to the AP, and therefore assign user traffic to the appropriate VSC. For this to work, the AP must be configured to send its SSID as the NAS ID in all authentication and accounting requests. See *Working with third-party autonomous APs on page 14-6*.

Number of accounting sessions

Specify the maximum number of sessions for which the service controller will track accounting information.

Maximum accounting sessions

Specify the maximum number of accounting sessions that the service controller supports.

Authentication UDP port

Indicates the port the service controller uses for authentication. This port is always set to the standard value of 1812.

Accounting UDP port
Indicates the port the service controller uses for accounting. This port is always set to the standard value of 1813.

Server authentication support

Select the authentication protocols that the internal RADIUS server will support:

- PAP: This protocol must be enabled if any VSCs are configured to use MAC-based authentication or HTML authentication.
- EAP-TTLS
- EAP-PEAP
- EAP-TLS

RADIUS authorization

Note Applies to autonomous and third-party APs. Requests from controlled APs are always accepted because they use the management tunnel.

Enable this option to restrict access to the RADIUS server. The RADIUS server will only respond to requests from RADIUS clients that appear in the list, or that match the default shared secret, as described below.

IP address
Specify the IP address of the RADIUS client.

Mask
Specify the network mask.

Shared secret
Specify the secret (password) that RADIUS client must use to communicate with the RADIUS server.

Default shared secret

Note Applies to autonomous APs only. Requests from controlled APs are always accepted because they use the management tunnel.

Enable this option to set a shared secret to safeguard communications between the internal RADIUS server and clients not in the RADIUS authorization list.

Shared secret/Confirm shared secret

Specify the secret (password) that service controller will use when communicating with RADIUS clients that do not appear in the RADIUS authorization list. The shared secret must match on both the clients and the service controller.

User account configuration

User accounts for the internal RADIUS server are defined using the **Service Controller >> Users** menu. See *Chapter 7: User authentication*.

Using a third-party RADIUS server

The service controller can use one or more RADIUS servers to perform a number of authentication and configuration tasks, including the tasks shown in the table below.

Task	For more information see
Validating administrative user credentials	*Administrative user authentication on page 4-4*.
Validating user credentials for 802.1X, MAC, and HTML authentication types	*Wireless protection on page 2-13.* *HTML-based user logins on page 2-17.* *MAC-based authentication on page 2-18.*
Storing custom configuration settings for the public access interface	*Chapter 9: Working with public access attributes*.
Storing custom configuration settings for each user	
Storing accounting information for each user	

Configuring a RADIUS server profile on the service controller

The service controller enables you to define a maximum of 16 RADIUS profiles. Each profile defines the settings for a RADIUS client connection. To support a client connection, you must create a client account on the RADIUS server. The settings for this account must match the profile settings you define on the service controller.

For backup redundancy, each profile supports a primary and secondary server.

The service controller can function with any RADIUS server that supports RFC 2865 and RFC 2866. Authentication occurs via authentication types such as: EAP-MD5, CHAP, MSCHAP v1/v2, PAP, EAP-TLS, EAP-TTLS, EAP-PEAP, EAP-SIM, EAP-AKA, EAP-FAST, and EAP-GTC.

Caution

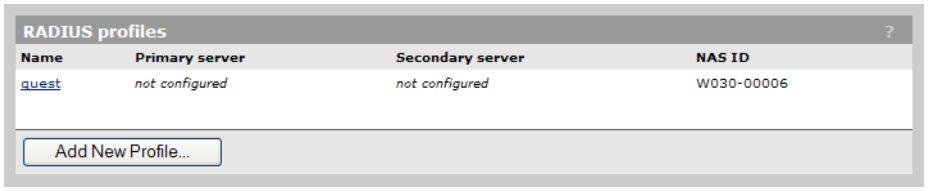
To safeguard the integrity of the RADIUS traffic, it is important that you protect communications between the service controller and the RADIUS server. The service controller lets you use PPTP or IPSec to create a secure tunnel to the RADIUS server. For complete instructions on how to accomplish this, see *Securing wireless client sessions with VPNs on page 12-3*.

Note

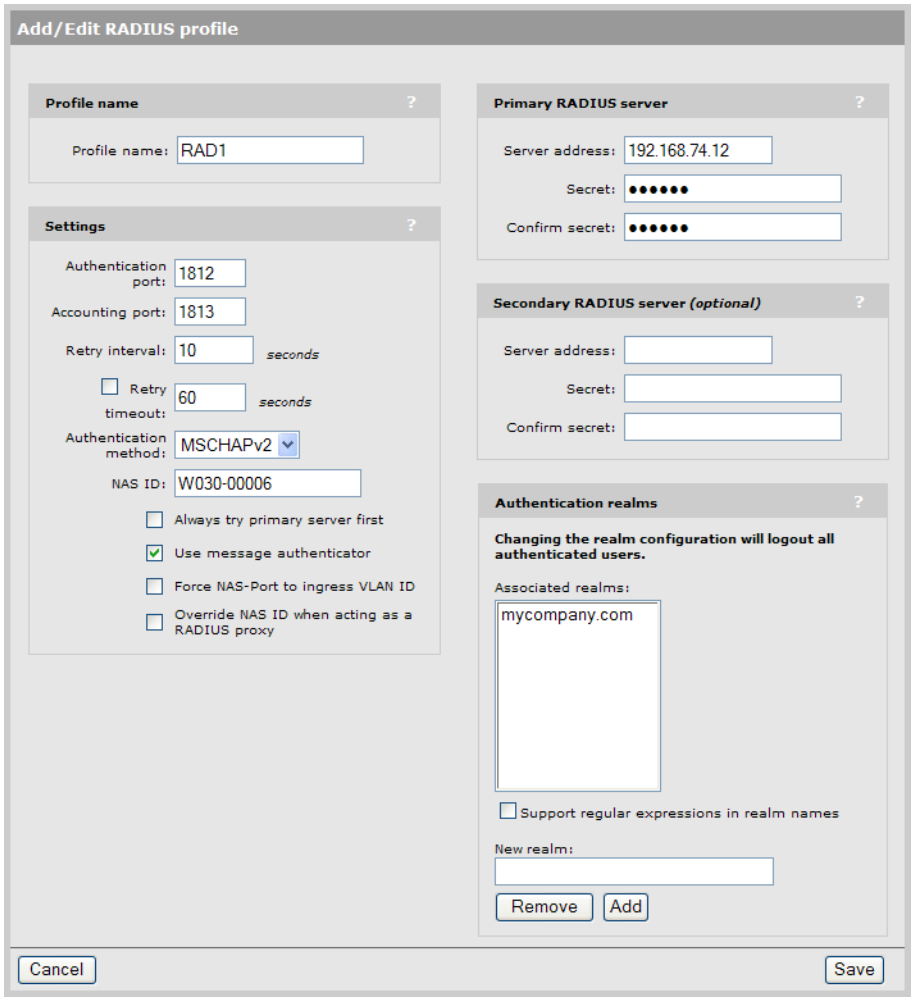
If you change a RADIUS profile to connect to a different server while users are active, all RADIUS traffic for active user sessions is immediately sent to the new server.

Configuration procedure

1. Select **Service Controller >> Authentication > RADIUS profiles.** The RADIUS profiles page opens.



2. Select **Add New Profile.** The Add/Edit RADIUS Profile page opens.



3. Configure the profile settings as described in the following section.
4. Select **Save**.

Configuration parameters

Profile name

Specify a name to identify the profile.

Settings

- **Authentication port:** Specify a port on the RADIUS server to use for authentication. By default RADIUS servers use port 1812.
- **Accounting port:** Specify a port on the RADIUS server to use for accounting. By default RADIUS servers use port 1813.
- **Retry interval:** Specify the number of seconds that the RADIUS server waits before access and accounting requests time out. If the server does not receive a reply within this interval, the service controller switches between the primary and secondary RADIUS servers, if a secondary server is defined. A reply that is received after the retry interval expires is ignored.

  Retry interval applies to access and accounting requests that are generated by the following:

  - Manager or operator access to the management tool
  - User authentication by way of HTML
  - MAC-based authentication of devices
  - Authentication of the service controller
  - Authentication of the controlled AP.

  You can determine the maximum number of retries as follows:

  - HTML-based logins: Calculate the number of retries by taking the setting for the HTML-based logins **Authentication Timeout** parameter and dividing it by the value of this parameter. Default settings result in 4 retries (40 / 10).
  - MAC-based and service controller authentication: Number of retries is infinite.
  - 802.1X authentication: Retries are controlled by the 802.1X client software.
- **Authentication method:** Select the default authentication method that the service controller uses when exchanging authentication packets with the RADIUS server defined for this profile. For 802.1X users, the authentication method is always determined by the 802.1X client software and is not controlled by this setting. If traffic between the service controller and the RADIUS server is not protected by a VPN, it is recommended that you use either EAP-MD5 or MSCHAP V2 (if supported by your RADIUS Server). PAP and MSCHAP V1 are less secure protocols.
- **NAS ID:** Specify the identifier for the network access server that you want to use for the service controller. By default the serial number of the service controller is used. The service controller includes the NAS-ID attribute in all packets that it sends to the RADIUS server.
- **Always try primary server first:** Enable this option if you want to force the service controller to contact the primary server first.

  Otherwise, the service controller sends the first RADIUS access request to the last known RADIUS server that replied to any previous RADIUS access request. If the request times out, the next request is sent to the other RADIUS server if defined.

For example, assume that the primary RADIUS server was not reachable and that the secondary server responded to the last RADIUS access request. When a new authentication request is received, the service controller sends the first RADIUS access request to the secondary RADIUS server.

If the secondary RADIUS server does not reply, the service controller retransmits the RADIUS access request to the primary RADIUS server. When two servers are configured, the service controller always alternates between the two.

Primary/Secondary RADIUS server

- **Server address:** Specify the IP address of the RADIUS server.
- **Secret/Confirm secret:** Specify the password for the service controller to use to communicate with the RADIUS server. The shared secret is used to authenticate all packets exchanged with the server, proving that the packets originate from a valid/ trusted source.

Authentication realms

When authentication realms are enabled for a profile, selection of the RADIUS server to use for authentication is based on the realm name, rather than the RADIUS profile name configured. This applies to any VSC authentication setting that uses the profile.

- Realm names are extracted from user names as follows: if the username is **person1@mydomain.com** then **mydomain.com** is the realm. The authentication request is sent to the RADIUS profile with the realm name **mydomain.com**. The username sent for authentication is still the complete **person1@mydomain.com**.
- For added flexibility, regular expressions can be used in realm names, enabling a single realm name to match many users. For example, if a realm name is defined with the regular expression **^per.*** then all usernames beginning with **per** followed by any number of characters will match. The following usernames would all match:

  per123.biz
  per321.lan
  per1

Important

- You must enable the use of authentication realms for the VSC.
- Realms names are not case-sensitive and can be a maximum of 64 characters long.
- You can define a maximum of 200 realms across all RADIUS profiles. There is no limit to the number of realms that you can define for each RADIUS profile.
- Each RADIUS profile can be associated with one or more realms. However, a realm cannot be associated with more than one profile.
- A realm overrides the authentication RADIUS server only. The server used for accounting is not affected.

Note When realm configuration is changed in any way, all active user sessions are terminated.

Using an Active Directory server

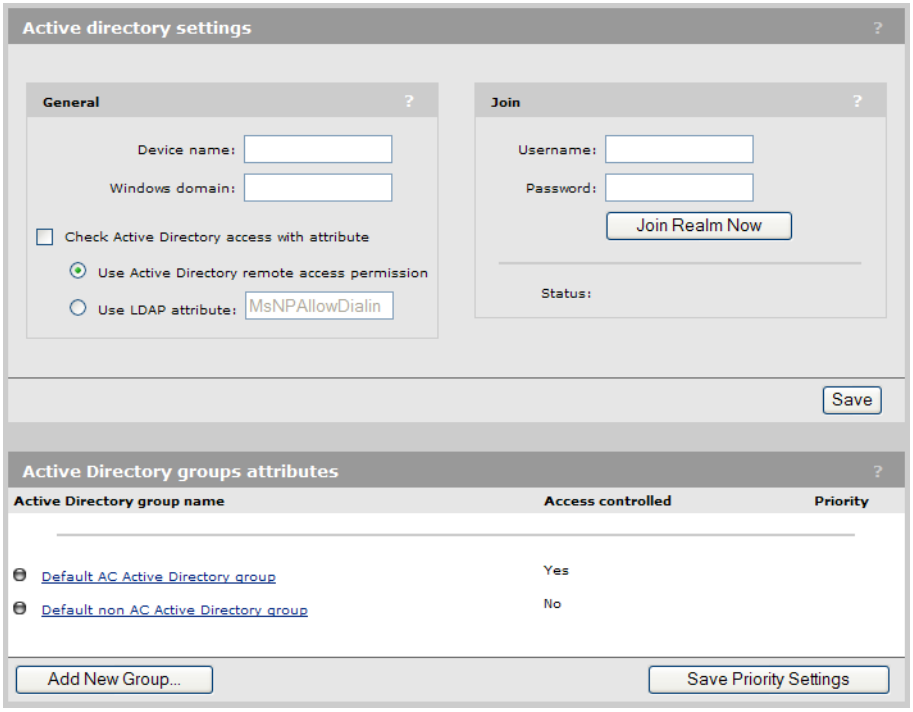
The service controller can be configured to validate user login credentials using an *external* Active Directory server for the following VSC features:

- Wireless Protection (only WPA and WPA2 both with EAP-PEAP)
- HTML-based logins.

Once a user is authenticated by Active Directory, the service controller retrieves the names of all the active directory groups of which the user is a member and uses them to activate appropriate configuration settings for the user locally-defined on the service controller.

Active Directory configuration

To configure active directory support, select **Service Controller >> Authentication > Active Directory**.



Active directory settings

General

Device name

Specify a name that identifies the service controller to Active Directory. The service controller uses this name to connect to the active directory server, just like any standard active directory client does.

Windows domain

Specify the Windows domain to which the service controller belongs. The service controller must be part of a Windows domain (**mydomain.com**, for example) to authenticate users that belong to that domain.

Check Active Directory access with attribute

Enable this option to have the service controller only accept users with a specific setting in their account.

- **Use Active Directory remote access permission:** Use the standard attribute defined in Active Directory for remote access (MsNPAllowDIalin). If this attribute is set, then the user can be authenticated via Active Directory.
- **Use LDAP attribute:** For non-standard implementation of Active Directory, set this according to the equivalent setting on the Active Directory server.

Join

Before the service controller can process user authentication using Active Directory, you must join the service controller with the Active Directory server. Fill in the required parameters and click **Join Realm Now**. This is usually a one-time event.

Username

Username the service controller will use to join Active Directory.

Password

Password the service controller will use to join Active Directory.

Note

For security reasons, **Username** and **Password** are not stored on the service controller.

Join Realm Now

Select to join the realm immediately.

Status

Shows the status of the join operation as follows:

- **Unknown:** System is processing, no status to report. Refresh the page to update the status.
- **DNS unavailable:** DNS not working, cannot access Active Directory.
- **Missing Config:** No configuration, so join cannot proceed.
- **Never Joined:** Administrator never selected **Join Realm Now**.
- **Not joined:** Not joined: May be joined with the domain, but the join is not confirmed yet. Status will change to **Joined** once confirmed. If the **Not Joined** status persists, check connectivity between the service controller and Active Directory or re-join.
- **Joined:** Active Directory reports that service controller successfully joined.

Active Directory groups attributes

Displays all Active Directory groups that are defined on the service controller. These groups are used to assign attributes to a user once they have been authenticated by Active Directory.

Note

Group names on the service controller must be identical to existing Active Directory Organizational Units configured on the Active Directory Server.

Once a user is authenticated by Active Directory, the service controller retrieves the names of all the active directory groups of which the user is a member.

- If the user is a member of only one Active Directory group, and that group name appears in the list, the service controller applies the attributes from that group.
- If the user is a member of more than one Active Directory group, the service controller applies the attributes from the matching group name with the highest priority (highest in the list).
- If no match is found, the attributes defined for one of the default groups are applied as follows:
  - If the VSC the user logged in on is access-controlled then the **Default AC Active Directory** group is used.
  - If the VSC the user logged in on is not access-controlled then the **Default non AC Active Directory** group is used.

Note

The default groups are disabled by default. You need to enable them before they can be used.

Add New Group

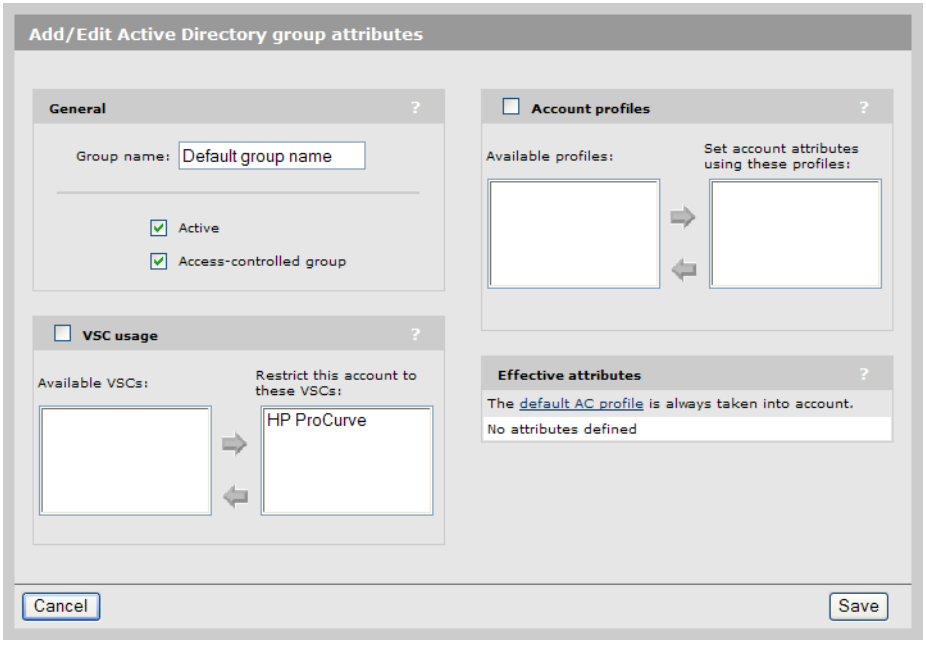
Select to add a new group. See *Configuring an Active Directory group on page 6-12*.

Save Priority Settings

After using the up/down arrows to change the priority of groups, save your changes by selecting this button.

Configuring an Active Directory group

An active directory group defines the characteristics of a user session. To make group configuration easy, account profiles (*Account profiles on page 7-6*) can be applied to set group attributes.



Configuration parameters

General

Group name

Specify a name to identify the group. This name must match an existing Active Directory Organizational Unit configured on the Active Directory Server.

Active

Enable this option to activate the group. The group cannot be used until it is active.

Access-controlled group

Determines whether the group is access-controlled or not.

- Access-controlled groups can only be used to log in on VSCs that are access-controlled.
- Non access-controlled groups can only be used to log in on VSCs that are not access-controlled.

VSC usage

Enable this option to restrict this group to one or more VSCs. If the selected VSCs are not defined on an AP, users will not be able to log in on this account.

The **Available VSCs** list shows all defined VSCs that you can select from.

To move VSCs between the two lists:

- Double-click the profile you want to move.
- Or, select the profile you want to move and then click the left or right arrow.

Account profiles

Enable this option to set the attributes of this group using one or more account profiles.

The **Available profiles** list shows all defined profiles that you can select from. To add a new profile, open the **Service Controller >> Users > Account profiles** page.

To move profiles between the two lists, double-click the profile you want to move, or select the profile you want to move and then select the left or right arrow.

Effective attributes

This list shows all attributes that are active for this Active Directory group. Each time you add an account profile for use by this group, all attributes configured in the profile are added to the **Effective attributes** list.

Note

Each profile that is applied to a group must have a unique set of attributes. The same attribute cannot be present in two different account profiles.

About the Default AC profile

The **Default AC profile** is always present and is always applied to all Active Directory groups. You can use this profile to add additional attributes that are not configurable in an account profile. Instead, these attributes are configured on the **Service Controller >> Public access > Attributes** page. Once added there, they will automatically appear in the **Effective attributes** list.

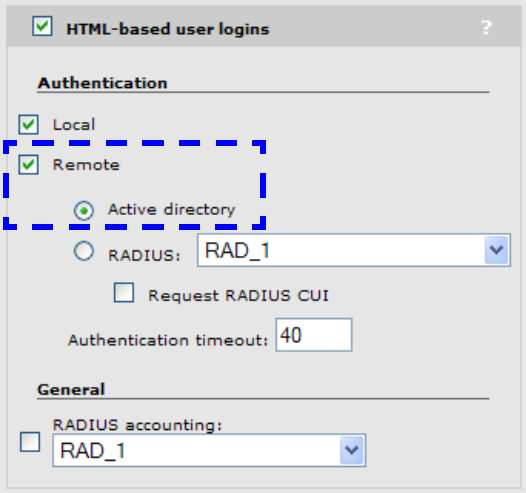
The following attributes can be added using this method:

Attribute	For information, see
default-user-use-access-list	*Access list on page 9-30*
default-user-welcome-url	*Default user URLs on page 9-52.*
default-user-goodbye-url	*Default user URLs on page 9-52.*
default-user-one-to-one-nat	*Default user one-to-one NAT on page 9-50.*
default-user-idle-timeout	*Default user idle timeout on page 9-49.*
default-user-session-timeout	*Default user session timeout on page 9-51.*
default-user-acct-interim-update	*Default user interim accounting update interval on page 9-48.*
default-user-max-output-packets	*Default user quotas on page 9-49.*
default-user-max-input-packets	*Default user quotas on page 9-49.*
default-user-max-total-packets	*Default user quotas on page 9-49.*

Attribute	For information, see
default-user-max-output-octets	*Default user quotas on page 9-49.*
default-user-max-input-octets	*Default user quotas on page 9-49.*
default-user-max-total-octets	*Default user quotas on page 9-49.*
default-user-max-input-rate	*Default user data rates on page 9-50.*
default-user-max-output-rate	*Default user data rates on page 9-50*
default-user-bandwidth-level	*Default user bandwidth level on page 9-49.*
default-user-use-public-ip-subnet	*Default user public IP address on page 9-51.*

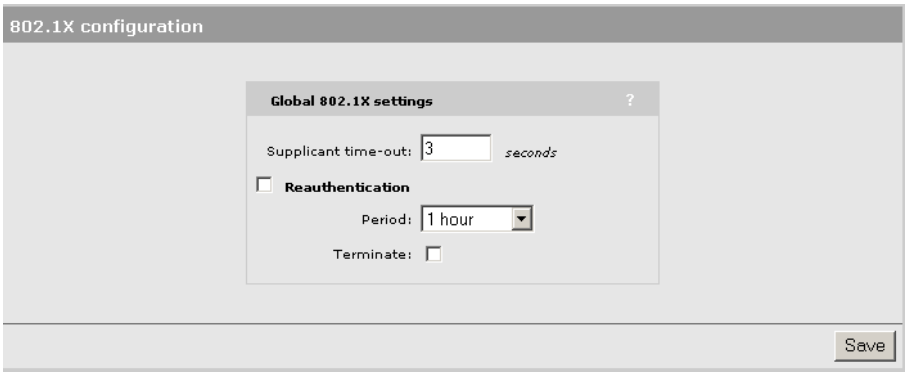
Configuring a VSC to use Active Directory

Any VSC feature that can be configured to support remote authentication can be configured to use Active Directory. For example, with HTML logins.



Configuring global 802.1X settings

The service controller provides several 802.1X settings that apply globally to all 802.1X connections. To configure these settings, select **Authentication > 802.1X**.



Configurable parameters on the **802.1X configuration** page include the following:

- **Supplicant timeout:** Specify the maximum length of time the service controller will wait for a client station to respond to an EAPOL packet before resending it.

  If wireless client stations are configured to manually specify the 802.1X username or password, or both, increase the value of the timeout to between 15 and 20 seconds.

- **Reauthentication**: Enable this option to force 802.1X clients to reauthenticate after the specified **Period**. This option is disabled by default.
  - **Period**: Client stations must reauthenticate after this amount of time has passed since their last reauthentication.
  - **Terminate**: Specifies how client traffic is handled during reauthentication.
    - **Disabled**: Client stations remain connected during reauthentication and traffic is blocked only if reauthentication fails.
    - **Enabled**: Client traffic is blocked during reauthentication and is activated again only if authentication succeeds.

Configuring MAC lists

MAC lists can be used by the switch ports on an MSM317 to restrict access to specific devices based on their MAC addresses.

For information on using MAC lists and filtering with respect to the MSM317, see the *MSM317 Access Device Installation and Getting Started Guide*.

7

User authentication

Contents

Key concepts 7-2
- Authentication support on a service controller 7-2
- Authentication support on a controlled AP 7-2
- Authentication types 7-3

Locally-defined user accounts 7-5
- Features 7-5
- Defining a user account 7-9
- Defining account profiles 7-11
- Defining subscription plans 7-13
- Accounting persistence 7-14

Key concepts

Note

This chapter discusses user authentication as it applies to controlled APs only. For information on working with autonomous APs, see *Chapter 14: Working with autonomous APs*.

User authentication tasks can be handled either by the AP or by the service controller. This is controlled by the settings of the access control and authentication options set on the VSC to which a user is assigned. See *About access control and authentication on page 2-6*.

Authentication support on a service controller

The following authentication types are supported on the service controller for both wired and wireless clients (except where noted):

- 802.1X (Wired 802.1X users can only be supported on the default VSC profile if access control is enabled. 802.1X wired users can be supported on other VSCs only if the 802.1X RADIUS Access Request contains a VLAN-Id indication using the Colubris VSA.)
- MAC-based (wireless users only)
- HTML-based (Wired HTML-based users can only be supported on the default VSC profile if access control is enabled. Wired HTML-based users on a VLAN can be supported on any VSC profile as long as access control is enabled and the appropriate VLAN is defined as the VSC ingress.)
- VPN-based (Wired VPN-based users can only be supported on the default VSC profile if access control is enabled. Wired HTML-based users on a VLAN can be supported on any VSC profile as long as access control is enabled and the appropriate VLAN is defined as the VSC ingress.)

The service controller can validate user login credentials using the local user list (integrated RADIUS server), a third-party RADIUS server, or an external Active Directory service. For information on configuring these options:

Authentication server	See
Integrated RADIUS server	*Locally-defined user accounts on page 7-5*. *Firewall on page 5-2*.
Third-party RADIUS server	*Using a third-party RADIUS server on page 6-5*.
Active Directory	*Using an Active Directory server on page 6-9*.

Authentication support on a controlled AP

The following authentication types are supported on a controlled AP for wireless clients only:

- 802.1X
- MAC-based

The AP can validate user login credentials using either the service controller or a third-party RADIUS server. Access-controlled VSCs always use the service controller for all user authentication tasks.

Authentication types

This section describes each authentication type.

802.1X authentication

Full support is provided for users with 802.1X or WPA / WPA2 client software that uses the following:

- EAP-TLS: Extensible Authentication Protocol Transport Layer Security.
- EAP-TTLS: Extensible Authentication Protocol Tunnelled Transport Layer Security.
- PEAP: Protected Extensible Authentication Protocol.

The group key can be changed at a specific interval.

Note For security reasons, use of 802.1X without enabling dynamic WEP encryption is not recommended.

MAC-based authentication

Devices can be authenticated based on their MAC address. This is useful for authenticating devices that do not have a Web browser (cash registers, for example).

There are two types of MAC-based authentication: global MAC and VSC-based MAC.

Global MAC	VSC-based MAC
Supported on the service controller only.	Supported on both service controller and AP.
Applies to both wired and wireless client stations.	Applies to wireless client stations only.
Applies to all VSCs that have HTML-based user authentication enabled. Authentication server is defined on a per-VSC basis however.	Customizable on a per-VSC basis.

User credentials can be validated using either a local user accounts, a third-party RADIUS server, or Active Directory. If more than one option is active, the local accounts are always checked first.

Global MAC

You can define global MAC-based authentication settings using the Colubris-AVPair value string `mac-address`, which you must add to the RADIUS account for the service controller. See *MAC authentication on page 9-53*.

Although the global MAC-based authentication settings apply to all VSCs that have HTML-based user authentication enabled, each VSC can use a different authentication server to validate user credentials. To define an authentication server for each VSC, open the **Add/ Edit Virtual Service Community** page and use the **HTML-based user logins** box to select the authentication method.

VSC-based MAC

Each VSC can have unique settings for media access control (MAC) authentication of wireless client stations. Support for RADIUS accounting is also configurable for each VSC. See *Working with VSCs on page 2-1*.

HTML-based authentication

This option provides support for users to log in with a Web browser via the public access interface provided by the service controller.

VPN-based authentication

This option defines settings for users who log in to the public access interface using a VPN connection. To use this option, one of the following VPN features must be enabled and configured on the **Service controller >> VPN** menu: L2TP server, PPTP server, or IPSec.

Important

- If you enable this option for a VSC, all wireless users on the VSC must establish a VPN connection. All other authentication methods (HTML, MAC) cannot be used.
- If you enable this option on the default VSC, all wired users must establish a VPN connection. (Wired users always connect to the default VSC.)
- When configuring user VPN software, the address of the VPN server is the one assigned to the service controller LAN port.

No authentication

For applications where a remote device performs all authentication functions, it can be useful to disable authentication on the service controller and instead, forward all traffic on a VSC into an egress GRE tunnel or egress VLAN for authentication by the remote device.

Note

Because the service controller routes traffic to the VSC egress, L2 information from the user is lost and only L3 information is available to the remote authentication device.

Filters

Input filters are available that enable you to control wireless access based on the IP or MAC address of client stations. These filters are configurable at the VSC level.

For information see:

- *Wireless MAC filter on page 2-19.*
- *Wireless IP filter on page 2-20.*

Locally-defined user accounts

The service controller provides support for locally-defined user accounts with a wide range of customizable options. Locally-defined user accounts use the integrated RADIUS server. Configuration of these accounts is done using the options on the **Service Controller >> Users** menu, which includes the following configuration pages: User accounts, Account profiles, Subscription plans, and Session persistence.

Each user account:

- Obtains account properties from one or more **account profiles**.
- Obtains account durations from one or more **subscription plans**.
- Is restricted for use with one or more **VSCs**.

Features

Access control

Two types of local user accounts are available: access-controlled and not access-controlled.

- Access-controlled accounts must be used with a VSC that is configured to provide access control.
- Non access-controlled accounts must be used with a VSC that is *not* configured to provide access control. These accounts are used to handle authentication directly at the AP and cannot not involve the access control capabilities of the service controller (the service controller must not be in the traffic data path).

Validity and subscription plans

Each user account can be associated with a subscription plan that defines:

- The time period during which the account is available.
- The total amount of time a user can be online when logged in with the account.

VSC usage

User accounts can be restricted to specific VSCs. if a the specified VSC is not available, then the user will not be able to connect with the account.

Account profiles

An account profile is used to define a specific set of features for a user account. Multiple account profiles can be applied to a user account allowing the feature sets of each profile to be added to the account.

Note

Each profile that is applied to a user account must have a unique feature set. The same feature cannot be present in two different profiles.

About the Default AC profile

The **Default AC profile** is defined by default, and is always applied to all access-controlled user accounts. You can view the settings for the **Default AC profile** by clicking it in the profile list. However, you cannot edit any of its settings directly. All settings for this profile are defined by setting attributes on the **Service Controller >> Public access > Attributes** page.

Supported attributes

The **Public access > Attributes** page allows a wide variety of attributes to be defined. However, only attributes that pertain to user configuration are applied to the **Default AC profile**. This includes the following attributes:

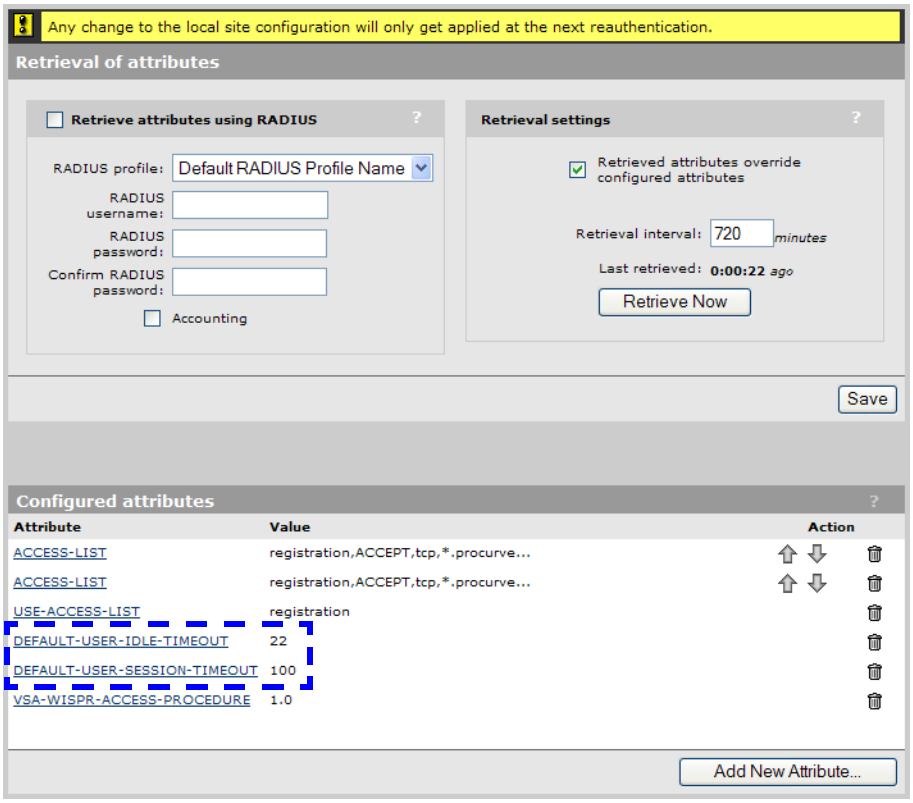
Attribute	For more info see
default-user-use-access-list	*Access list on page 9-30.*
default-user-welcome-url	*Default user URLs on page 9-52.*
default-user-goodbye-url	*Default user URLs on page 9-52.*
default-user-one-to-one-nat	*Default user one-to-one NAT on page 9-50.*
default-user-idle-timeout	*Default user idle timeout on page 9-49.*
default-user-session-timeout	*Default user session timeout on page 9-51.*
default-user-acct-interim-update	*Default user interim accounting update interval on page 9-48.*
default-user-max-output-packets	*Default user quotas on page 9-49.*
default-user-max-input-packets	*Default user quotas on page 9-49.*
default-user-max-total-packets	*Default user quotas on page 9-49.*
default-user-max-output-octets	*Default user quotas on page 9-49.*
default-user-max-input-octets	*Default user quotas on page 9-49.*
default-user-max-total-octets	*Default user quotas on page 9-49.*
default-user-max-input-rate	*Default user data rates on page 9-50.*

Attribute	For more info see
default-user-max-output-rate	*Default user data rates on page 9-50.*
default-user-bandwidth-level	*Default user bandwidth level on page 9-49.*
default-user-use-public-ip-subnet	*Default user bandwidth level on page 9-49*

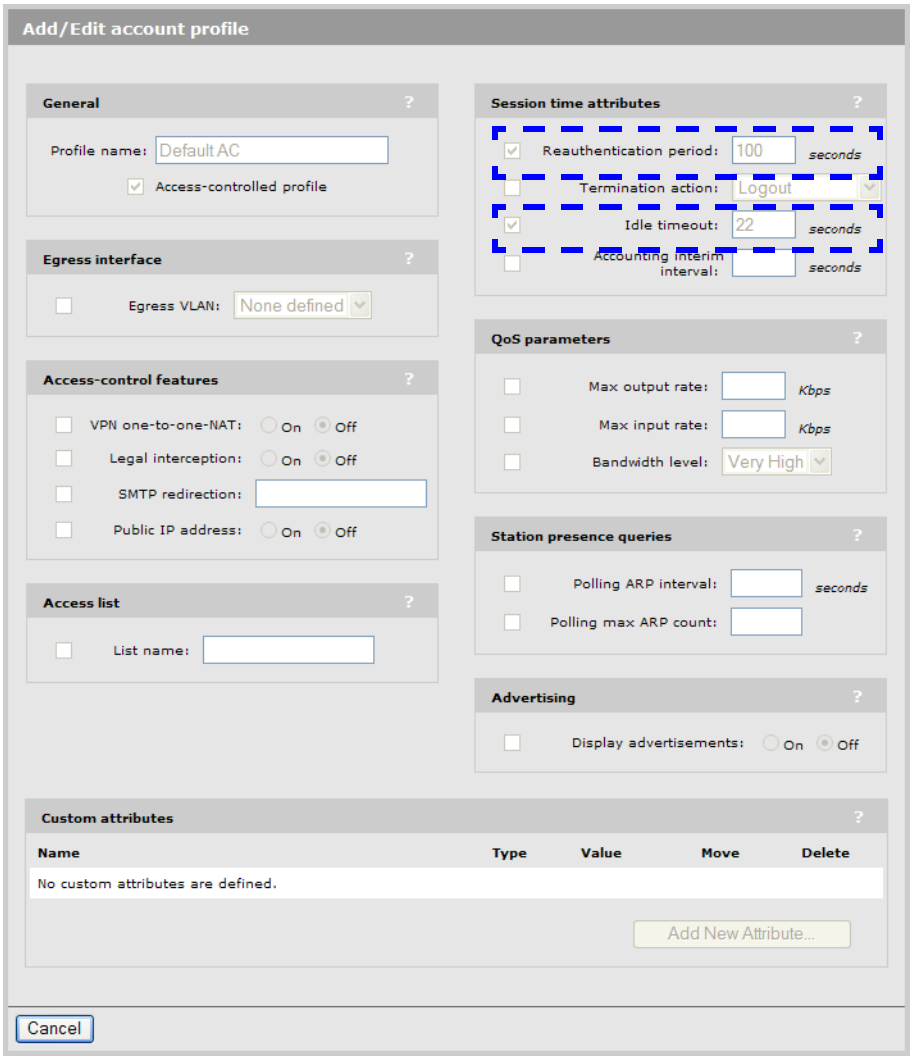
Example

This example illustrates how to indirectly customize the Default AC profile by defining several attributes, and shows how these settings are then reflected in a the Default AC profile and the user account.

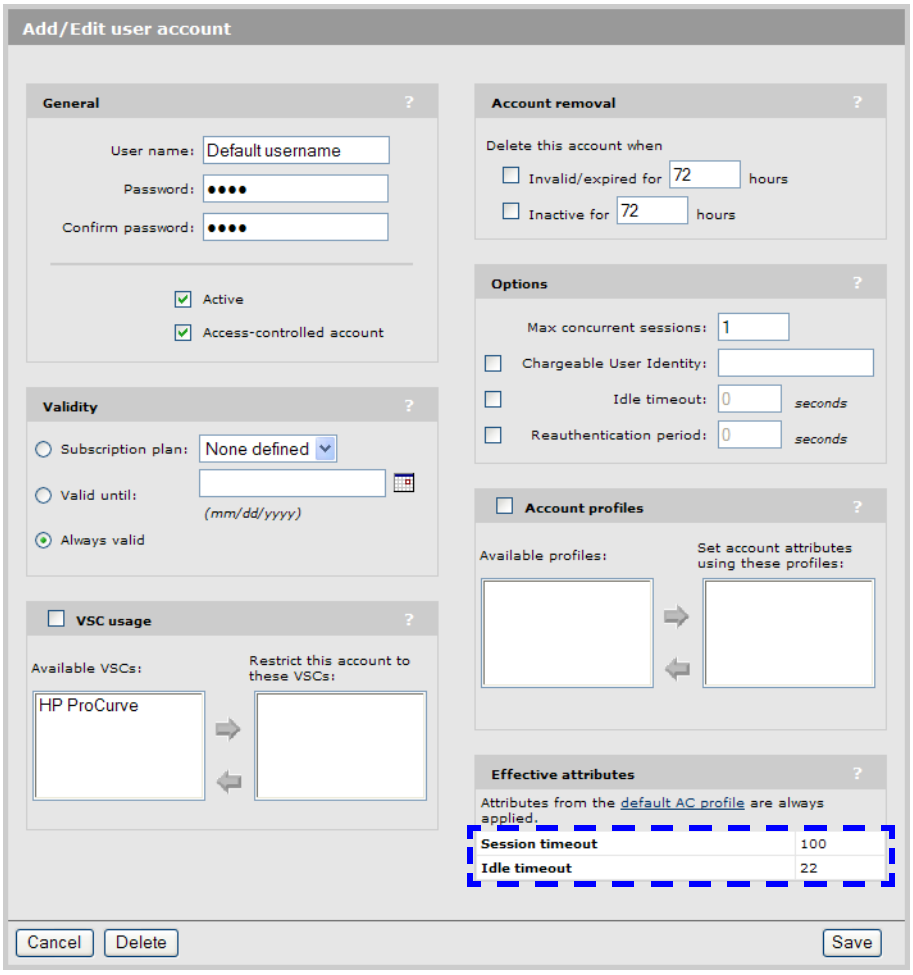
The following sample page shows several attributes defined on the **Public access > Attributes** page under **Configured attributes**. The two of interest for this example are highlighted below.



These two attributes appear in the **Default AC** profile under **Session time attributes**:

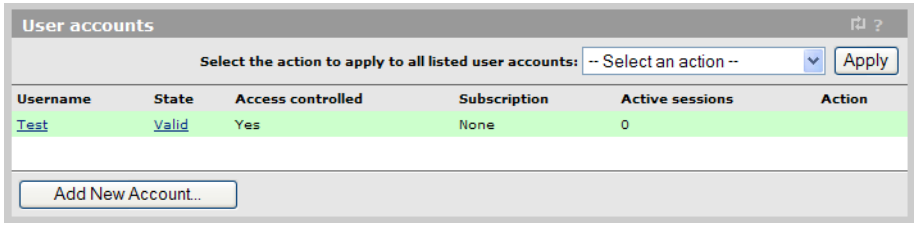


And the attributes appear in access-controlled user accounts under **Effective attributes**:

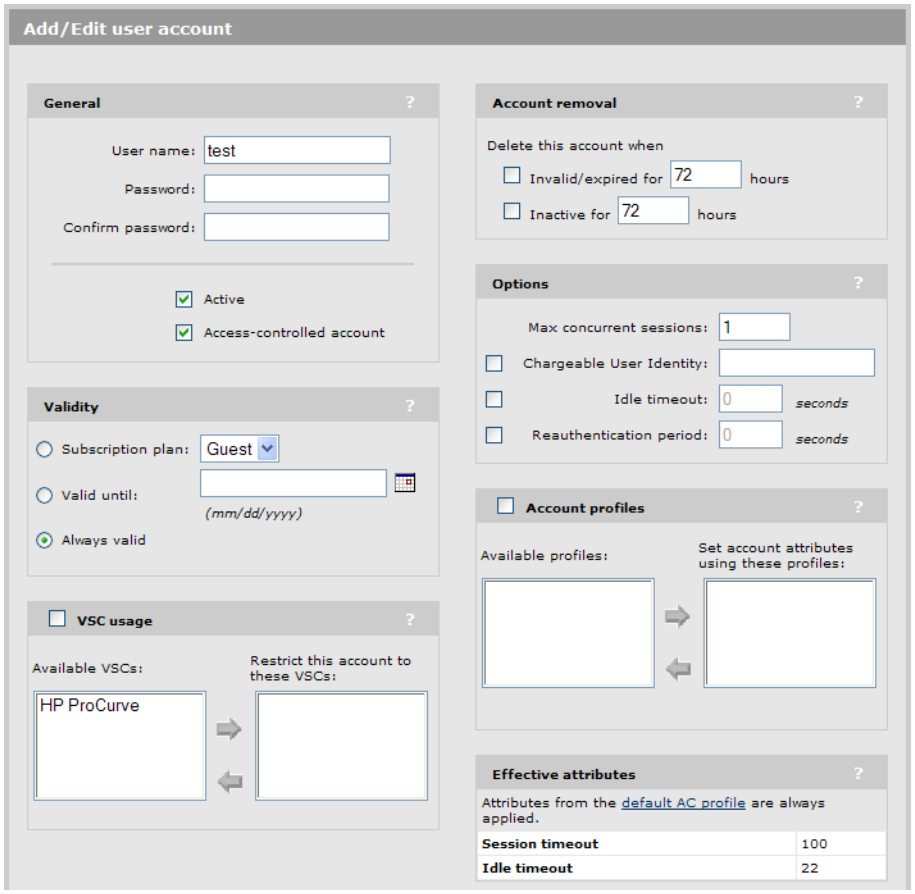


Defining a user account

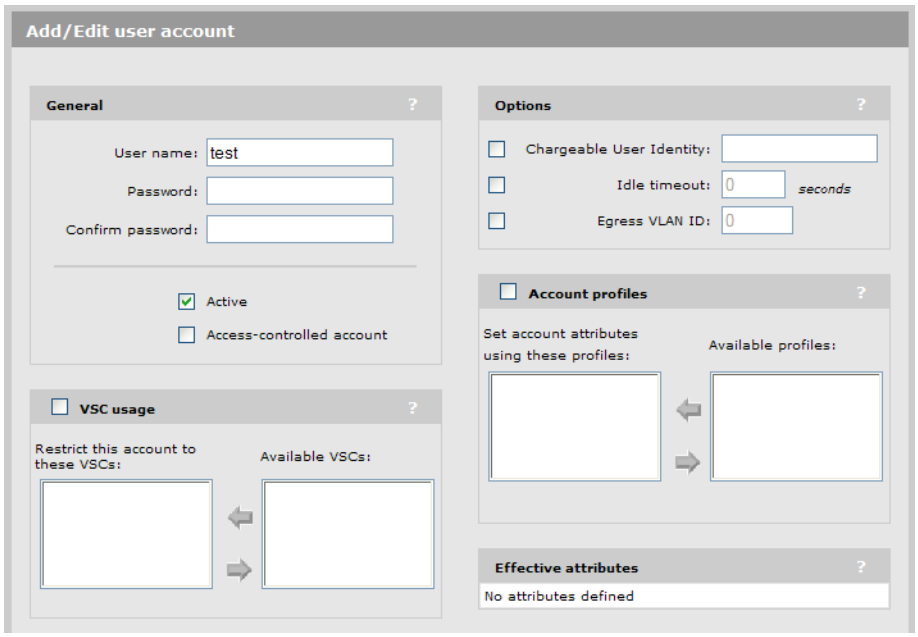
1. Select **Service Controller >> Users > User accounts**. The User accounts page opens. It presents a list of all defined user accounts. Initially this list is empty.


User accounts
Select the action to apply to all listed user accounts: -- Select an action -- Apply
Username State Access controlled Subscription Active sessions Action
Test Valid Yes None 0
Add New Account...

2. Select **Add New Account**. The **Add/Edit user account** page opens.



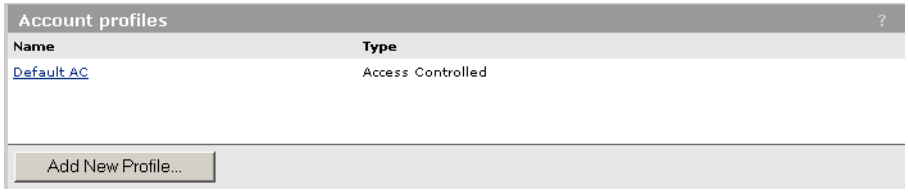
If you disable the Access-controlled account option, the page will look like this:



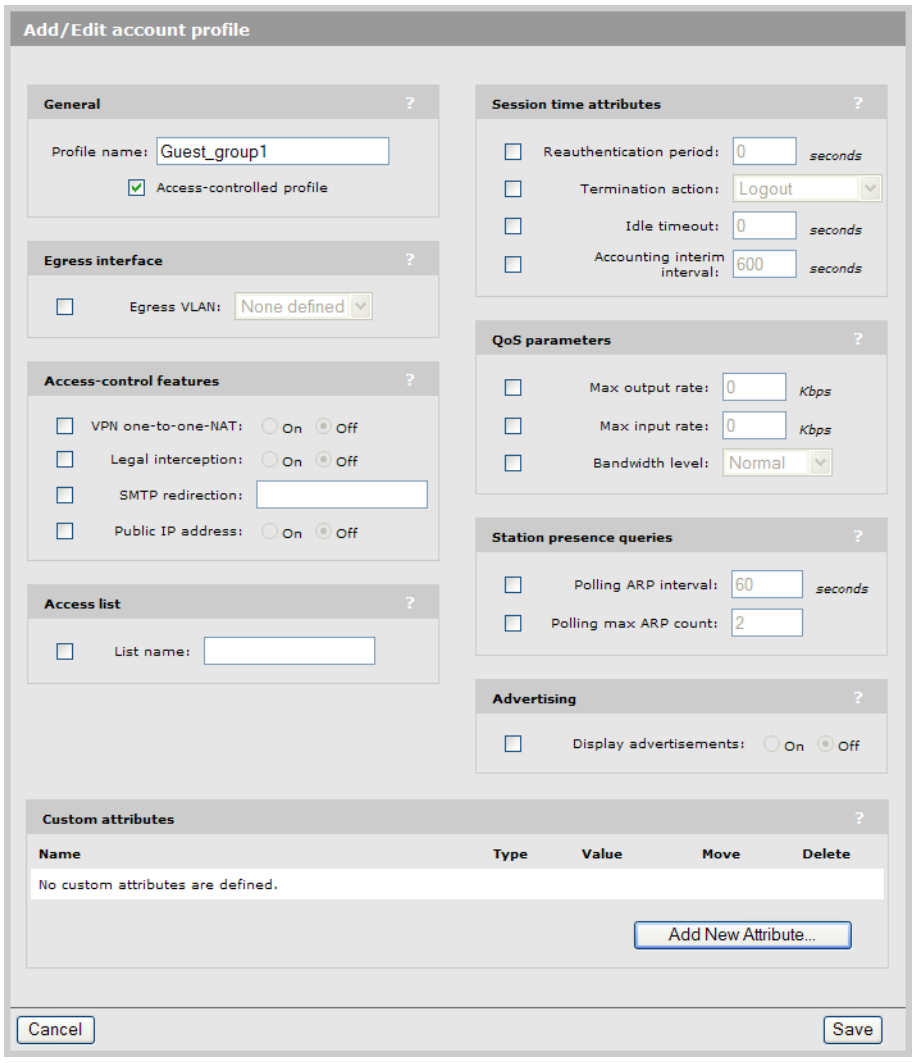
3. Configure account options as described in the online help.

Defining account profiles

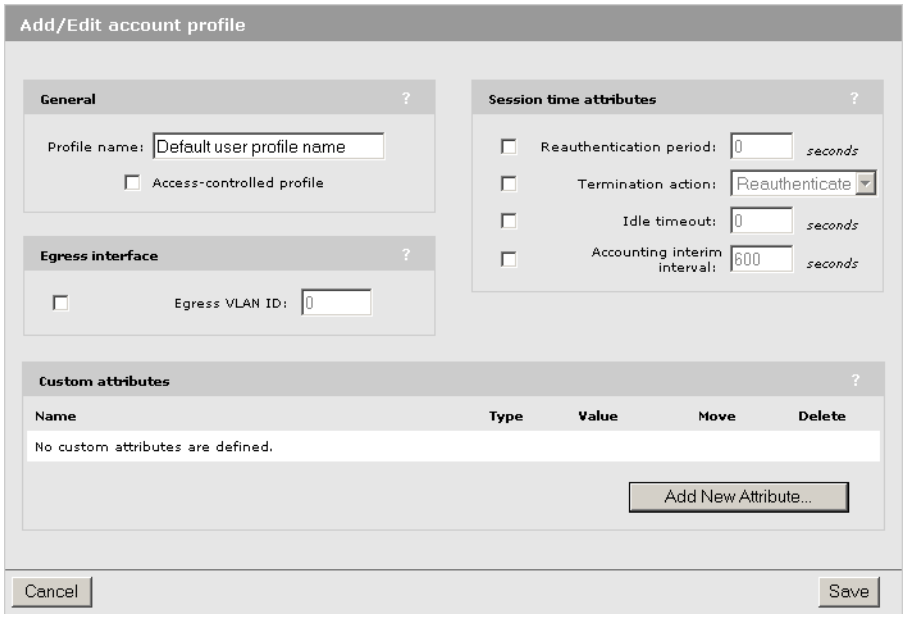
1. Select **Service Controller >> Users > Account profiles**. The Account profiles page opens. It presents a list of all defined profiles. Initially this list will contain the profile **Default AC**.



2. Select **Add New Profile**. The **Add/Edit account profile** page opens.



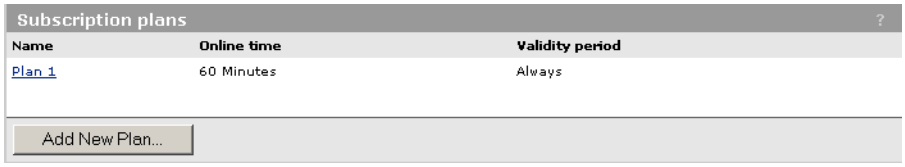
If you disable the Access-controlled account option, the page will look like this:



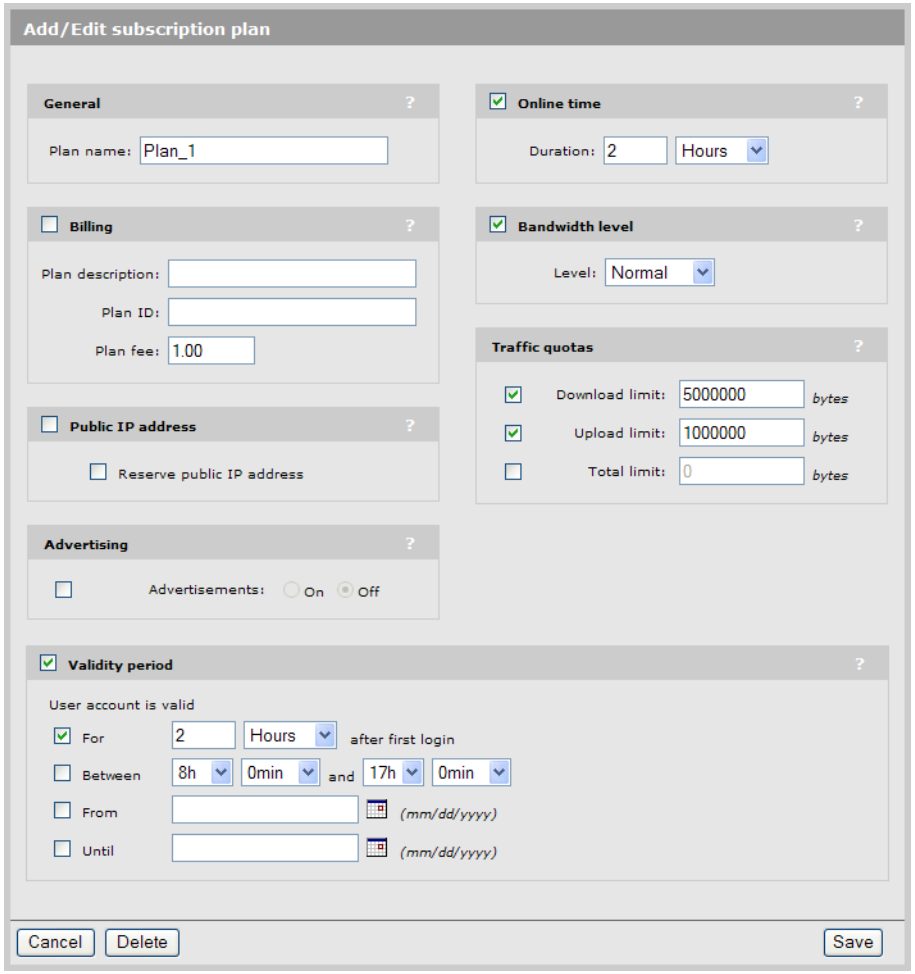
3. Configure profile options as described in the online help.

Defining subscription plans

1. Select **Service Controller >> Users > Subscription plans**. The Subscription plans page opens. It presents a list of all defined subscription plans.



2. Select **Add New Plan**. The Add/Edit subscription plan page opens.



3. Configure plan options as described in the online help. For an example, see *Defining a subscription plan for access purchase on page 8-8*.

Public IP address

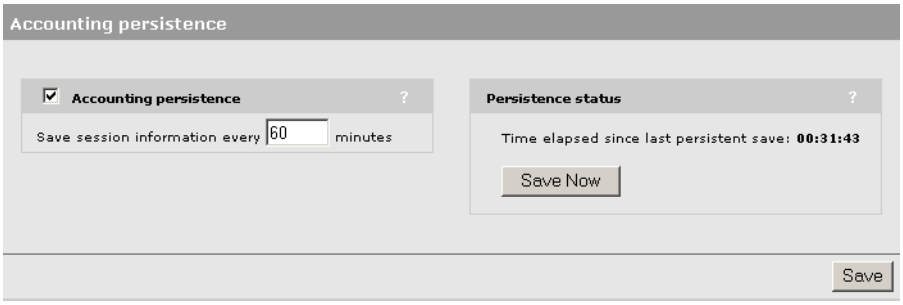
This feature enables a public IP address to be assigned to any client station. This makes the client station address visible to devices on the external network, allowing external devices to create connections with the client station.

The public IP address feature only works when the Internet port is set to static IP addressing. To configure the available public IP addresses, open the **Service controller >> Network > Ports > Internet port > Static addressing** page.

Accounting persistence

Enable this option to have the service controller save accounting information to its internal flash memory so that can be recovered in case of abnormal system shutdown. Restarting the service controller via its management tool (**Service Controller >> Maintenance > System**) saves before restarting.

The minimum save time is 30 minutes.



8

Public/guest network access

Contents

Key concepts....8-3
- About the public and protected networks....8-3
- About the public access interface....8-4
- Public access examples....8-4
- Default configuration....8-4

Public access interface tour....8-5
- About the “Subscribe to the service” feature....8-5
- About the “Use Free Access service” feature....8-8
- About the “Existing user” feature....8-8
- Displaying advertisements....8-10

Public access interface flow....8-11

Customizing the public access interface....8-12
- Common configuration tasks....8-13

Setting site configuration options....8-18
- Allow subscription plan purchases....8-18
- Display the Free Access option....8-19
- Support a local Welcome page....8-19
- Use frames when presenting ads....8-19
- Allow SSLv2 authentication....8-20
- Redirect users to the Login page via....8-20

Customizing public access interface Web pages....8-21
- Site file archive....8-21
- FTP server....8-21
- Current site files....8-22

Global access control settings....8-29
- Access control parameter definitions....8-30

Web server configuration 8-33
Options 8-33
Ports 8-34
MIME types 8-34
Security 8-35

Payment services 8-36
Payment services configuration 8-36
Service settings 8-36

Billing record logging 8-38
Settings 8-39
Persistence 8-40
External billing records server profiles 8-40
Billing records log 8-43

Location-aware authentication 8-45
How it works 8-45
Example 8-47
Security 8-48

Key concepts

The *Public/Guest Network Access* feature enables the service controller to provide controlled network access for a variety of deployments. Some common applications of this feature are:

- Providing Internet access to wireless customers in airports, restaurants, train stations, conference halls, etc.
- Providing wireless and wired access to staff and guests in hospitals, corporations, government buildings.
- Providing wireless and wired access to students, staff, and teachers in schools and universities.
- Providing outdoor wireless access for an entire town, enabling city workers, police, fire, public security, and the general public to connect.

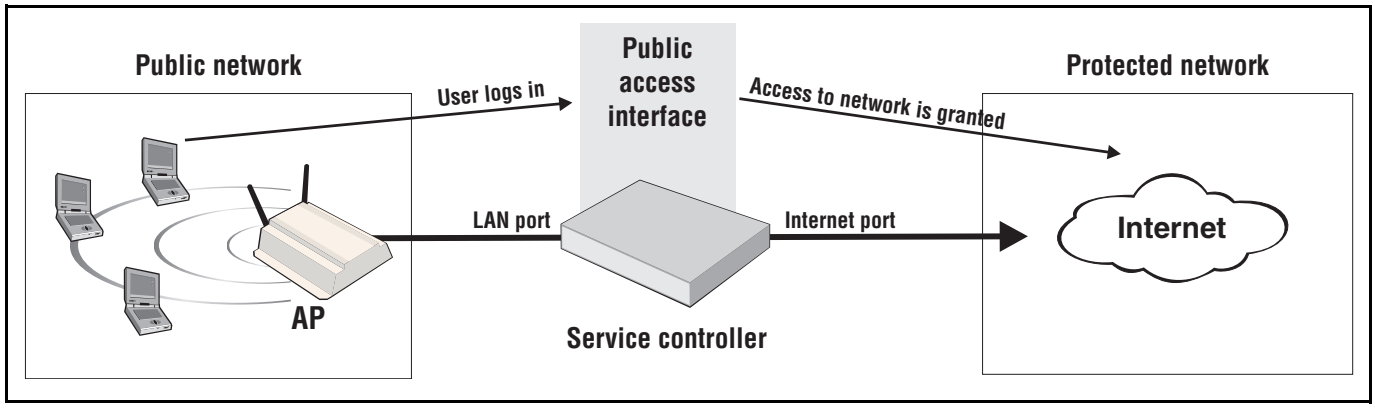
This chapter provides details on the public/guest network access feature and how it can be used. See also, *Chapter 9: Working with public access attributes on page 9-1*.

About the public and protected networks

In this type of deployment, the service controller acts as the gatekeeper between two distinct network segments: the public network and the protected network.

- Typically, access to the public network and its resources is available to all users once they successfully associate with the wireless network.
- Access to the private network is restricted by the service controller, and typically requires that users be authenticated by the service controller. In most cases, user login occurs with a Web browser via the public access interface Login page. The service controller can validate user login credentials using locally defined user accounts or by using the services of a third-party authentication server (RADIUS or Active Directory).

The following diagram shows the public and private networks for a simple public access deployment.



About the public access interface

The public access interface is the sequence of Web pages that users use to log in, log out, and view the status of their wireless connections to the public access network. By default, these Web pages are hosted on the service controller integrated Web server. However, pages can also be hosted on external servers for added flexibility.

Standard pages are provided for common tasks such as login, service purchase, and display of session information. The pages are all fully editable and customizable, enabling you to tailor the public access interface Web pages to provide a customized look-and-feel for your site.

Advertisements can be displayed at a specific interval if required.

Note The public access interface is only active on access-controlled VSCs.

Note If only MAC-based authentication is defined on the default VSC, wired users gain access to the network without being authenticated. Wireless users however, must log in because MAC-based authentication applies to wireless users only.

Public access examples

Sample public access files are referenced in this chapter. You can download a Public Access Examples zip file from the HP ProCurve manuals page at: **www.procurve.com/manuals**. Look under **MSM7xx Controllers**. Download the zip file and extract its content to a folder on your computer.

Default configuration

By default, the service controller creates a VSC named **HP ProCurve** with the following properties:

- Wireless network name: **HP ProCurve**
- **Use Service Controller for Authentication** is enabled. (If you disable this option, the service controller will not provide user authentication services for 802.1X, WPA, or WPA2.)
- **Use Service Controller for Access control** is enabled. (If you disable this option, you disable the public access interface and all users gain access to the protected network.)
- HTML-based authentication is enabled.

This means that when a user connects to the default VSC:

- Unauthenticated users cannot access the protected network, except for: procurve.com (for product registration) and windowsupdate.com (for IE which tries to get to a windows update on fresh start).
- Authenticated users *can access all* protected network resources.

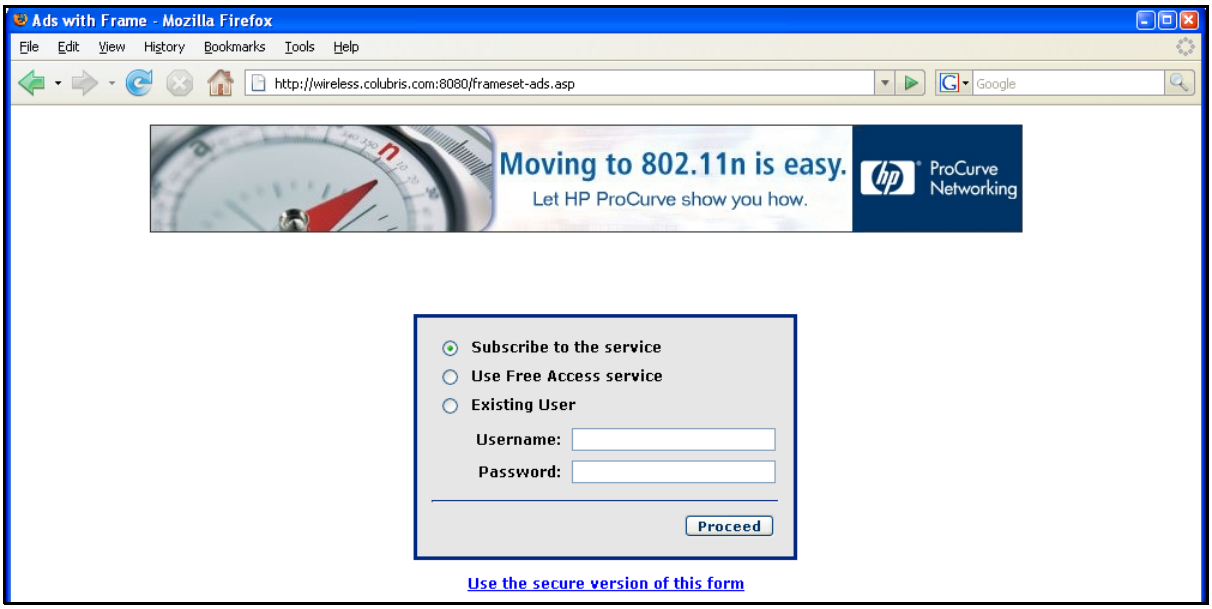
Note If authentication is not enabled on a VSC, all connected users can access the protected network.

Public access interface tour

The service controller includes a Web server that is used to host the Web pages that make up the public access interface. Standard pages are provided for common tasks such as login, subscription purchase, and display of session information. The pages, error messages, images, and workflow are all customizable. Advertisements can be displayed at a specific interval.

This tour of the public access interface shows the default public access interface pages, and some of the customization options available by selecting **Service Controller >> Public access > Web content > Site options**.

When a wireless user attempts to browse to a public Web site, they are temporarily redirected to the public access interface Login page shown below.



About the “Subscribe to the service” feature

When this feature is enabled, it allows first-time users to subscribe to the service by dynamically creating their own accounts, which includes setting the following:

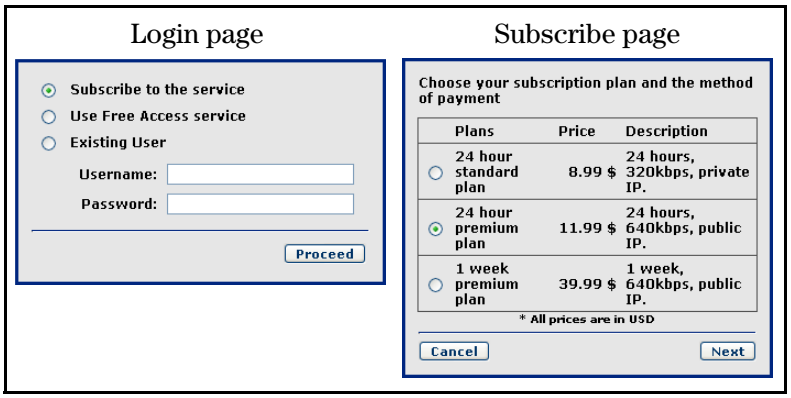
- username and password
- subscription plan
- payment method

Existing users can also select this option in order to change the subscription plan and billing method they are currently using.

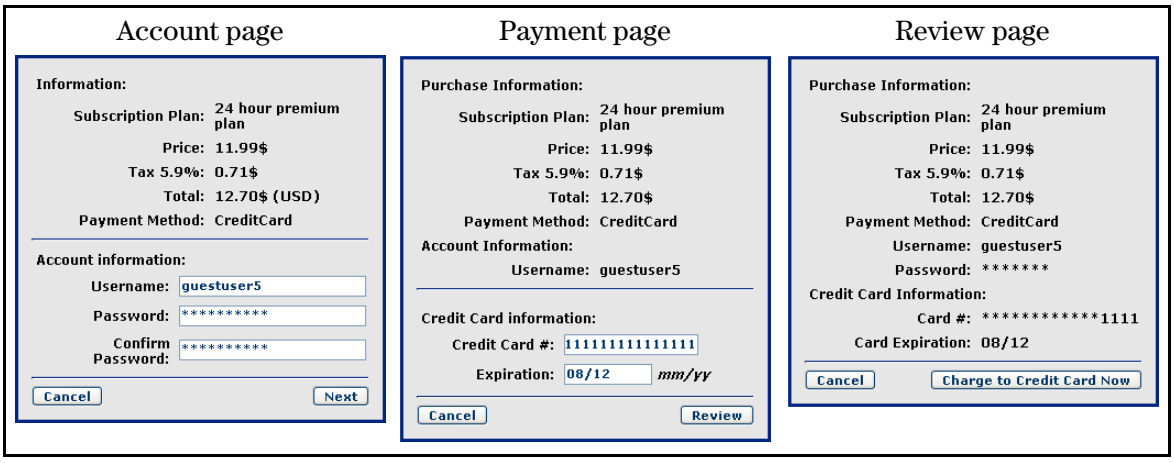
To configure this feature, see *Allow subscription plan purchases on page 8-18*.

The following steps illustrate the typical user experience when this feature is active.

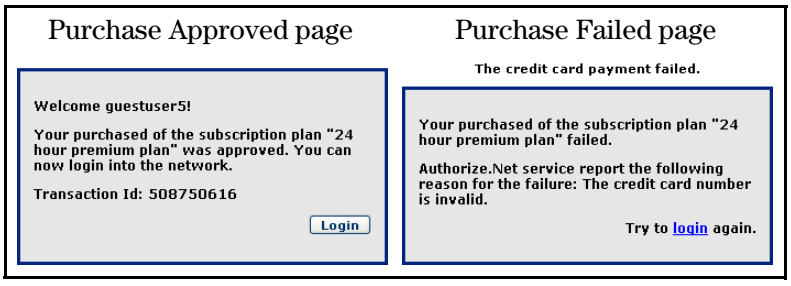
1. On the Login page, the user selects **Subscribe to this service** and clicks **Proceed**. On the Subscribe page, the user selects a subscription plan and clicks **Next**.



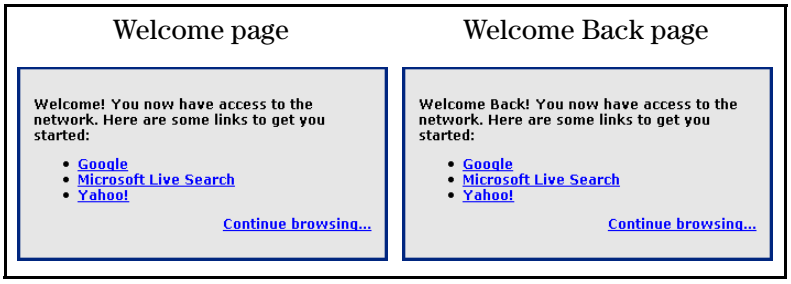
2. On the Account page, the user creates a new **Username** and **Password** and clicks **Next**. On the Payment page, the user enters payment information and clicks **Review**. Finally, the user reviews the purchase information, and clicks **Charge to Credit Card Now**. **Cancel** is available at each stage.



3. Purchase success or failure is indicated with an appropriate message.

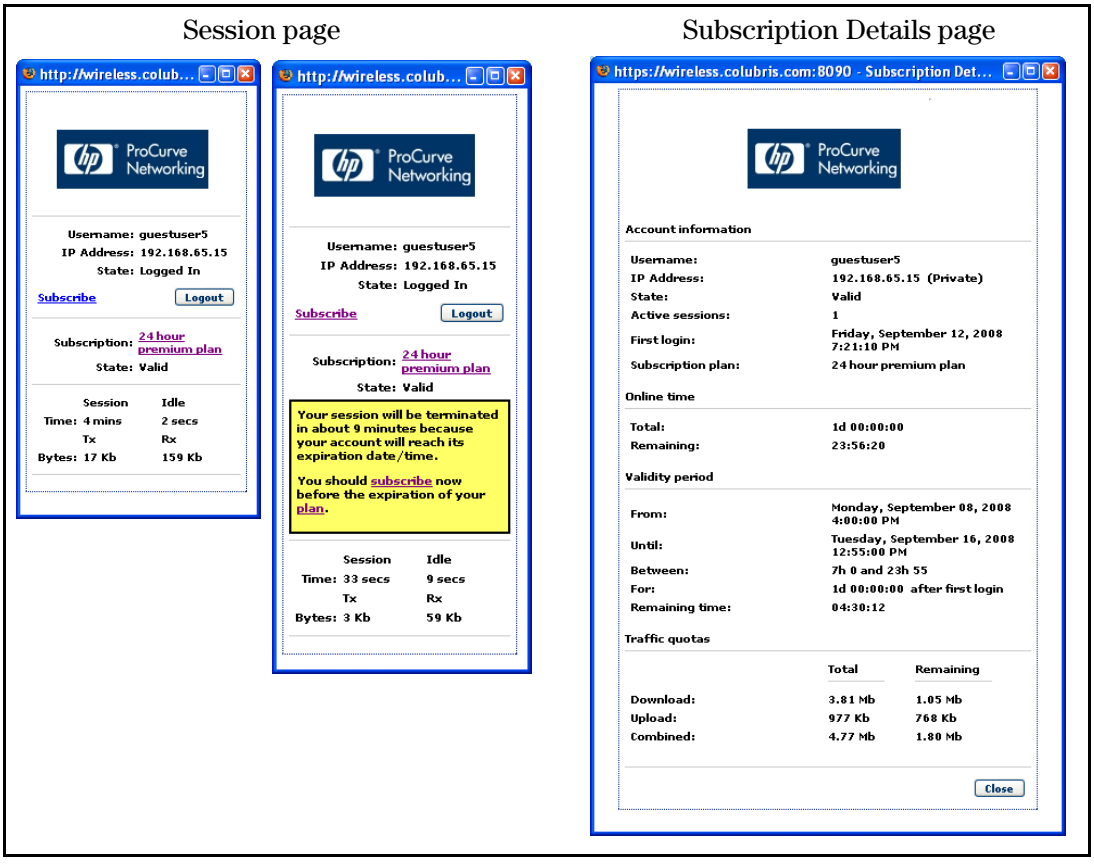

Purchase Approved page
Welcome guestuser5!
Your purchased of the subscription plan "24 hour premium plan" was approved. You can now login into the network.
Transaction Id: 508750616
Login
Purchase Failed page
The credit card payment failed.
Your purchased of the subscription plan "24 hour premium plan" failed.
Authorize.Net service report the following reason for the failure: The credit card number is invalid.
Try to login again.

4. After a successful purchase, the user clicks **Login**. The welcome page appears. The user can then click **Continue browsing** to launch the page that they originally requested, or click other links as desired.


Welcome page
Welcome Back page
Welcome! You now have access to the network. Here are some links to get you started:
Google
Microsoft Live Search
Yahoo!
Continue browsing...
Welcome Back! You now have access to the network. Here are some links to get you started:
Google
Microsoft Live Search
Yahoo!
Continue browsing...

Note that when enabled, and a user with a still-valid subscription re-connects to the network, they are automatically logged in and greeted with the Welcome back page.

5. As soon as the user has a successful login, a small session page also appears. When the subscription plan has only 10 minutes left, a warning appears encouraging the user to purchase another plan before their existing one expires. Detailed subscription plan information is available via the Session page subscription plan link.



About the “Use Free Access service” feature

This feature provides free access to any user. Users simply select this option and click **Proceed**. They can then browse freely without the need for a username or login.

To activate this feature, see *Display the Free Access option on page 8-19*.

About the “Existing user” feature

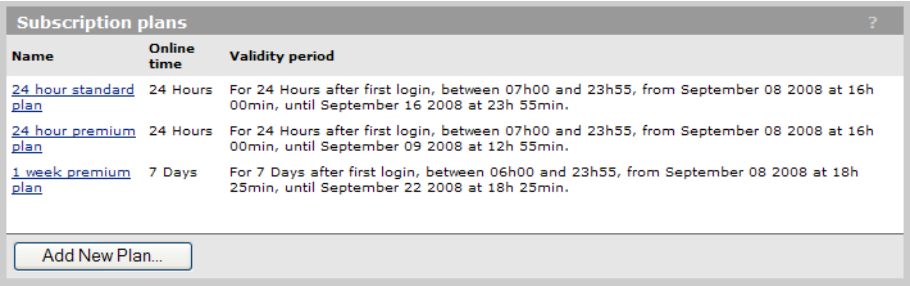
Users that already have an account, use this option to log in. These could be predefined accounts that were created by an administrator, or user-created accounts created via the **Subscribe to the service** feature.

You can use this option to support a prepaid model in which users purchase a network access voucher before logging in. To do this, you first need to create a suitable subscription plan and then define users (see *Locally-defined user accounts on page 7-5* or *Chapter 6: Authentication services on page 6-1*).

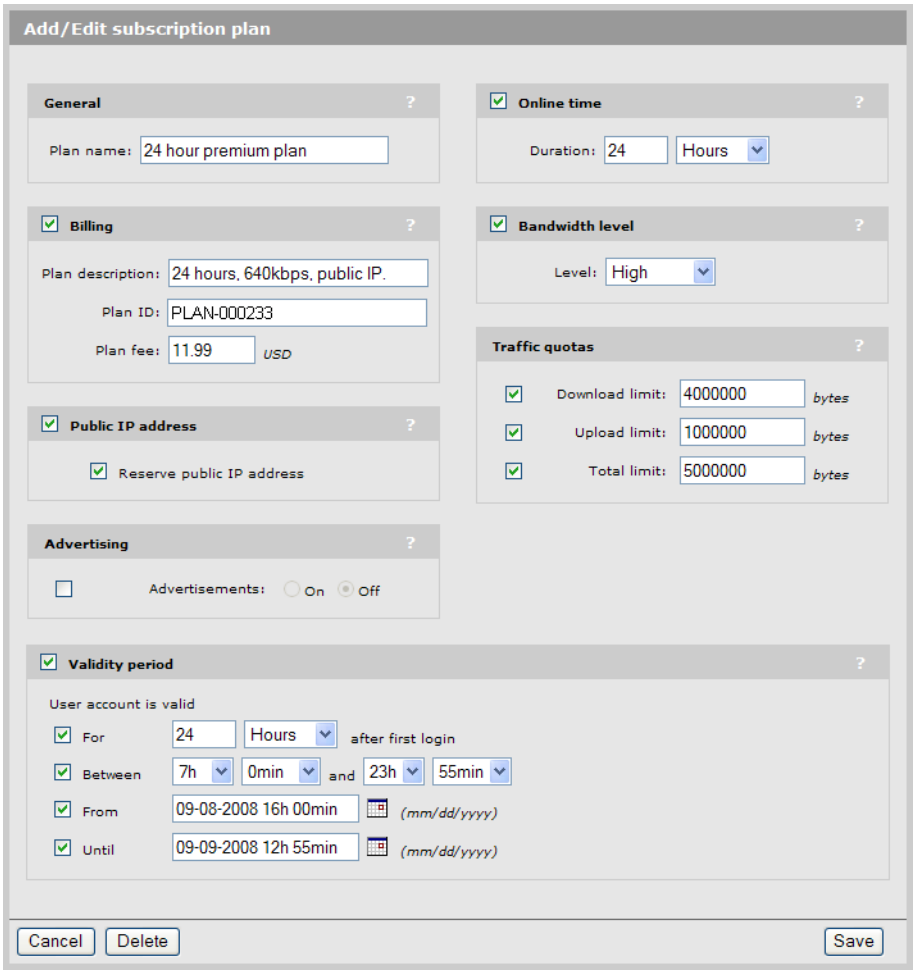
Users can then log in and use the service for as long as the subscription plan permits.

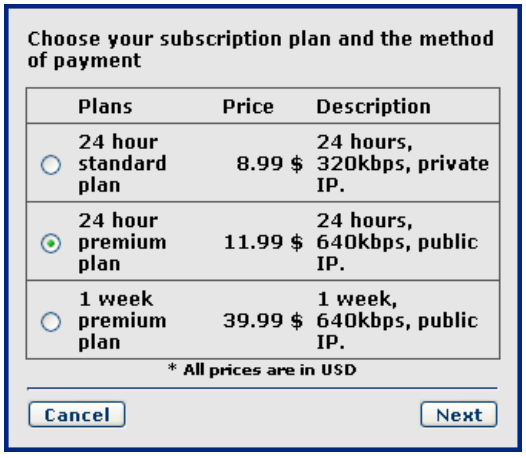
Defining a subscription plan for access purchase

Configure subscription plans by selecting **Service Controller >> Users > Subscription plans**.


Subscription plans
Name
Online time
Validity period
24 hour standard plan
24 Hours
For 24 Hours after first login, between 07h00 and 23h55, from September 08 2008 at 16h 00min, until September 16 2008 at 23h 55min.
24 hour premium plan
24 Hours
For 24 Hours after first login, between 07h00 and 23h55, from September 08 2008 at 16h 00min, until September 09 2008 at 12h 55min.
1 week premium plan
7 Days
For 7 Days after first login, between 06h00 and 23h55, from September 08 2008 at 18h 25min, until September 22 2008 at 18h 25min.
Add New Plan...

Select **Add New Plan** to add a plan or click a plan name to edit it. Be sure to enter a descriptive plan name, enable Billing, and include the Plan fee, and Validity period. For example, here is a plan definition and how it appears in the public access interface. See also, *Defining subscription plans on page 7-13*.



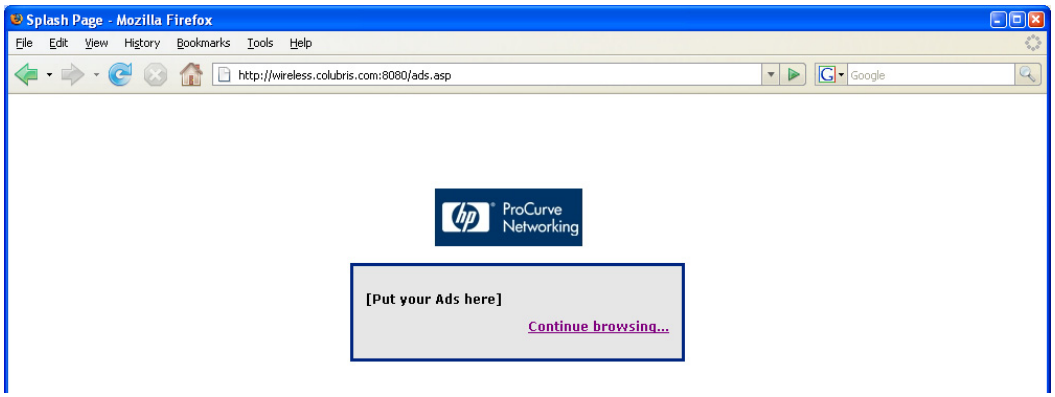


Displaying advertisements

When enabled, and the configured interval has elapsed, an administrator-defined advertisement is displayed either in a frame or on a separate page. For example:

- Logo and advertisement displayed in frame at top of page:

- Logo and advertisement displayed on separate page. User clicks **Continue browsing** to continue:



To display ads in a frame, enable **Service Controller > Public access > Access control> Display advertisements**. Optionally also set the display interval.

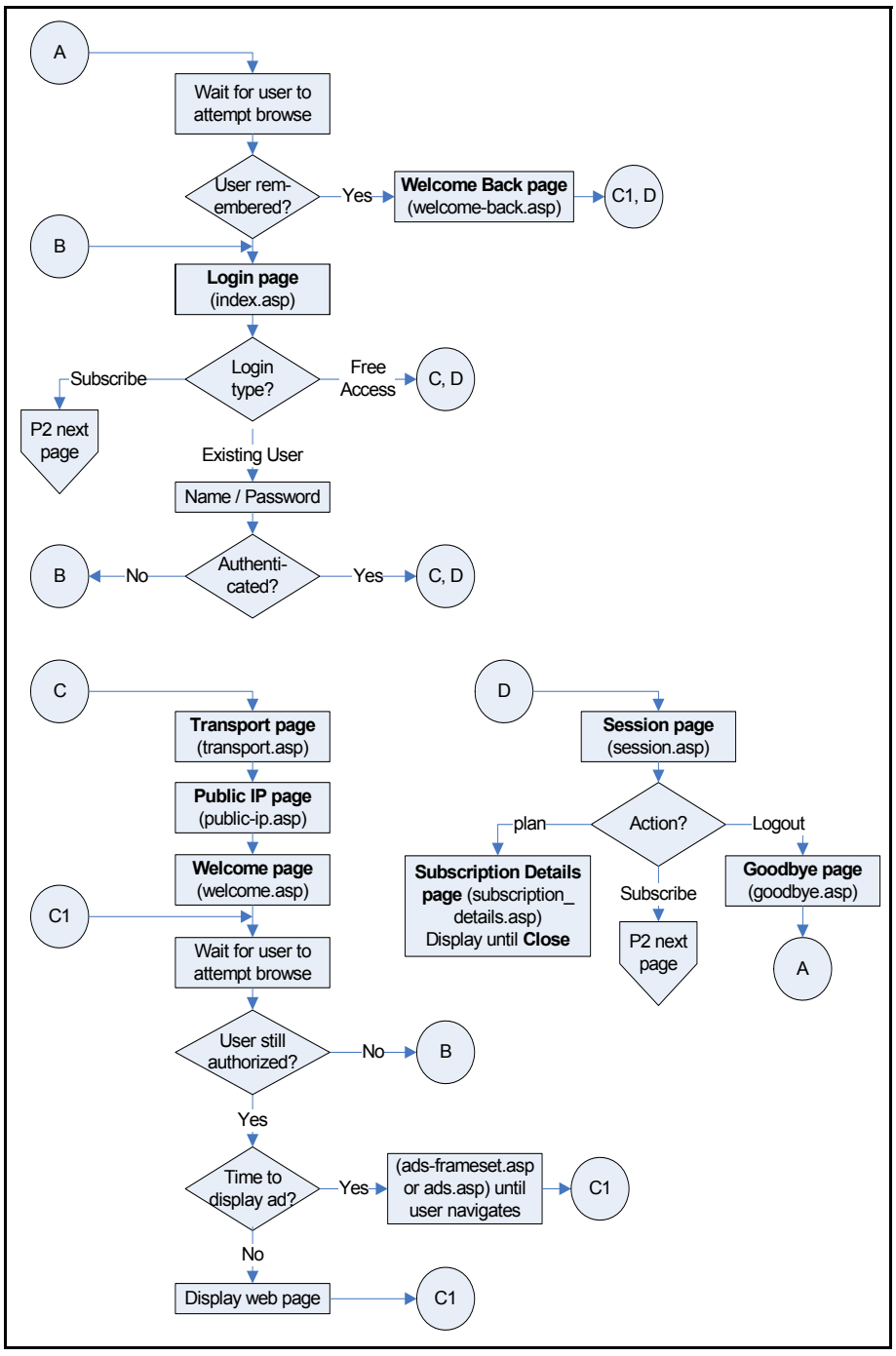
Note

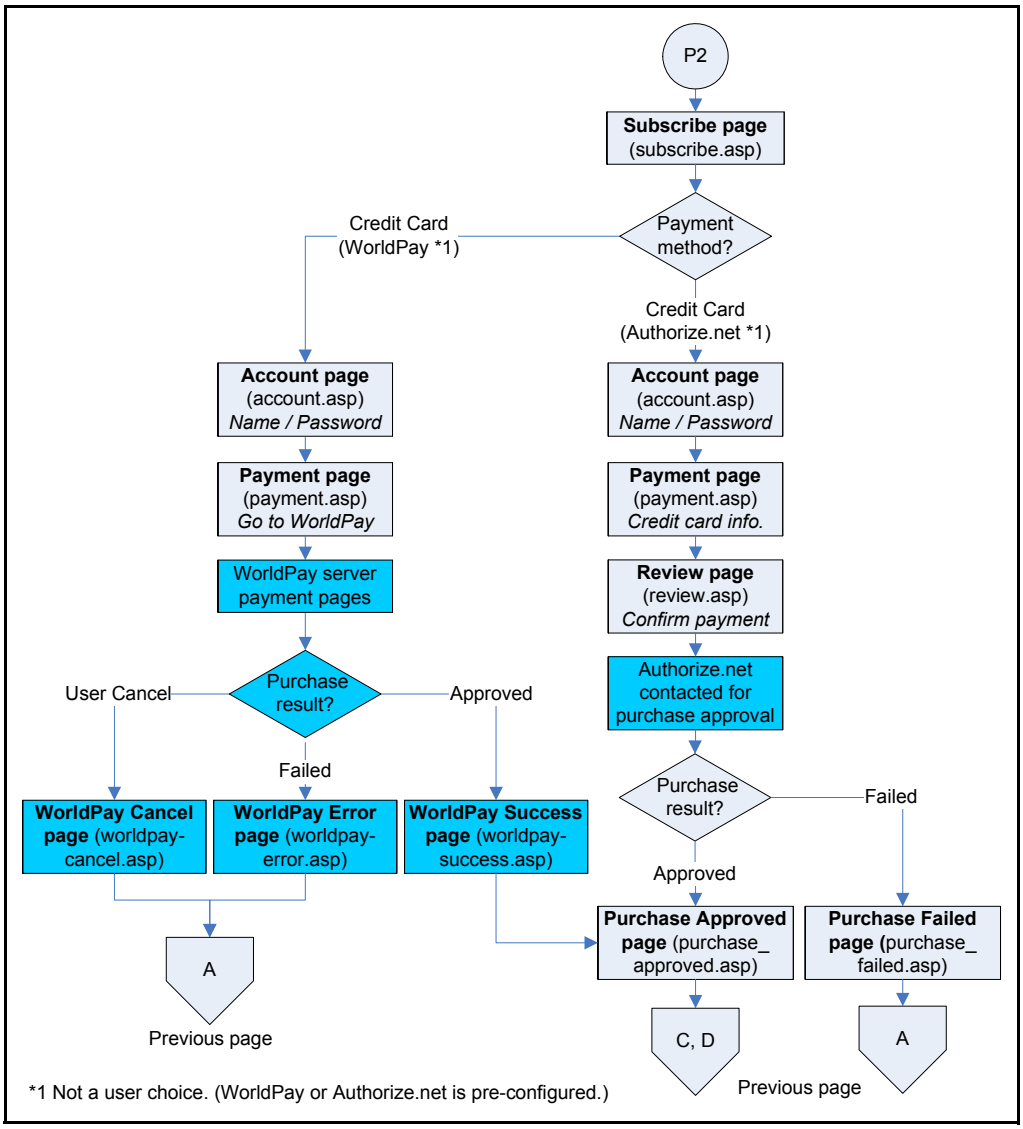
Once the **Display advertisements** option is enabled, advertisements are displayed for all users. You can selectively disable the display of advertising in user profiles (**Users > Account profiles**), subscription plans (**Users > Subscription plan**), or via attributes set in a user's RADIUS account.

Public access interface flow

The two following diagrams provide an overview of the default public access interface Web page flow. All site Web pages are identified by their role: **Login**, **Welcome**, **Logout**, etc. This abstraction is used because the name of the actual page used for a particular role is configurable in many cases. (For reference, the page name used by the factory default configuration is provided in parenthesis.)

For a description of the individual pages, see *Current site files on page 8-22*.





Customizing the public access interface

The public access interface can be customized using the methods described below. You might use one or more of these methods, depending on the type of customization that you want to perform.

- **Setting site configuration options:** The site configuration options on the **Service controller >> Public access > Web content** page can be used to quickly enable/disable certain public access features.

  See *Setting site configuration options on page 8-18*.

- **Customizing the public access interface Web pages:** The Web pages hosted on the service controller internal Web server can be modified, allowing the entire public access interface to be customized. Simple modifications can be made with basic knowledge of

HTML. Users with advanced HTML skills and knowledge of ASP and Javascript will be able to fully-customize all site operations.

See *Customizing public access interface Web pages on page 8-21*.

- **Setting public access attributes:** Configuration of a number of public access features can be accomplished by setting various RADIUS attributes. There categories of attributes are available:
  - **Site attributes:** These attributes are used to configure site-related options and global settings that apply to all user sessions. They can be defined in the RADIUS account for the service controller or reside locally on the service controller.

    See *Defining and retrieving site attributes on page 9-3*.
  - **User attributes:** These attributes are used to customize settings on a per-user basis. These attributes can reside locally on the service controller or be retrieved from a third-party RADIUS server.

    See *Defining and retrieving user attributes on page 9-5*.

Common configuration tasks

Customizing the login page

1. Select **Service Controller >> Public access > Web content.**
2. Under **Current site files**, click **index.asp**.
3. Edit **index.asp** to meet the requirements of your site.
4. Click **Save**.

Customizing the logo

1. Create a file called **logo.gif** that contains your logo (recommended size less than 20K).
2. Select **Service Controller >> Public access > Web content.**
3. Under **Current site files**, click the garbage can icon to the right of **logo.gif** to delete it.
4. Click **Add New File**.
5. For **Filename**, specify **logo.gif.**
6. Next to **Load content from file**, click **Browse**.
7. Select the **logo.gif** file that you created in Step 1.
8. Click **Load**.

Displaying custom welcome and goodbye pages

This example shows how to display unique welcome and goodbye pages for specific users or groups of users.

For this example, assume you have two sets of users: basic and premium. To distinguish the two groups, you have set up the user accounts on the RADIUS server accordingly. (Perhaps you are using access lists to restrict each group to a different section of the public network as described in *Access list example on page 9-37*).

1. Create the following two folders on your Web sever: **basic** and **premium**.
2. See *Public access examples on page 8-4*. Copy public access sample files **welcome.html** and **goodbye.html** into each both folders and customize them for each set of users.
3. Add the following entry to the RADIUS profile for the basic users.

   ```
   welcome-url=web_server_URL/basic/welcome.html
   goodbye-url=web_server_URL/basic/goodbye.html
   ```

4. Add the following entry to the RADIUS profile for the premium users.

   ```
   welcome-url=web_server_URL/premium/welcome.html
   goodbye-url=web_server_URL/premium/goodbye.html
   ```

5. Add the following entry to the RADIUS profile for the service controller. This gives all unauthenticated users access to the Web server hosting the goodbye page.

   ```
   access-
   list=loginserver,ACCEPT,tcp,web_server_IP_address,port_number
   ```

Delivering dynamically generated content

Another way to generate custom pages is to add placeholders in the URLs for the custom external pages and then use server-side scripting to dynamically create the pages. This method provides a powerful mechanism to automatically generate completely customized pages on a per-user basis. Rather than designing one or more static pages, as in the previous example, the custom pages in this example can be built on-the-fly based on user preferences stored in a central database, or based on a user's location within the network.

For example, if you want to generate a custom welcome page for each user:

1. Add the following entry to the RADIUS profile for the service controller.

   ```
   welcome-url=web_server_URL/premium/
   welcome.html?loginname=%u&IPaddress=%i
   ```

2. Create a server-side script to retrieve the user's login name (%u) and the service controller IP address or domain name (%u). The script can use this information to then display a custom page based on user's preferences (stored in the server database) and the user's location within the wireless network.

Supporting PDAs

Users using PDAs that only support a single browser window will have difficulty using the public access interface in its standard configuration.

Once a user logs in to the public access interface, two Web pages are sent to their browser: the Welcome page and the Session page.

The Session page contains a logout button. Users who are unable to view this page will not be able to log out.

To solve the problem, modify the Welcome page to include a logout button.

1. Create a folder called **PDAusers** on your Web sever.
2. See *Public access examples on page 8-4*. Copy public access sample files **welcome.html** and **goodbye.html** into the **PDAusers** folder.
3. Edit **welcome.html** to include a logout link with the target:

   `http://service controller_`*`name`*`:`*`port`*`/goform/HtmlLogout.`

   For example:

   `http://wireless.mycompany.com:8080/goform/HtmlLogout.`

   Adds a warning to this page that tells PDA users to bookmark the Welcome page so that they can logout.
4. Add the following entry to the RADIUS profile for all PDA users.

   `welcome-url=`*`web_server_URL`*`/PDAusers/welcome.html`

AV-Pair values for customizing pages

The following table lists the AV-Pair values that can be used to change individual pages. To change all pages as a group see *Loading custom pages from an archive on page 9-42*.

Web item	Default name	AV-Pair value	See . . .
Login	index.asp	login-page login-url	*Login page on page 9-43* *Use the following values to reference pages that reside on an external Web server. on page 9-44*
Welcome Back	welcome-back.asp	n/a	
Subscribe	subscribe.asp	n/a	
Transport	transport.asp	transport-page	*Transport page on page 9-43*
Public IP	public-ip.asp	session-page	
Welcome	welcome.asp	welcome-url	*Welcome page on page 9-44*
Session	session.asp		*Session page on page 9-43*
Ads	ads.asp or ads-frameset.asp	n/a	
Account	account.asp	n/a	
Payment	payment.asp	n/a	
Review	review.asp	n/a	
Purchase Approved	purchase-approved.asp	n/a	
Purchase Failed	purchase-failed.asp	n/a	
Goodbye	goodbye.asp	goodbye-url.asp	*Goodbye page on page 9-44*
Logo	logo.gif	logo	*Logo on page 9-43*

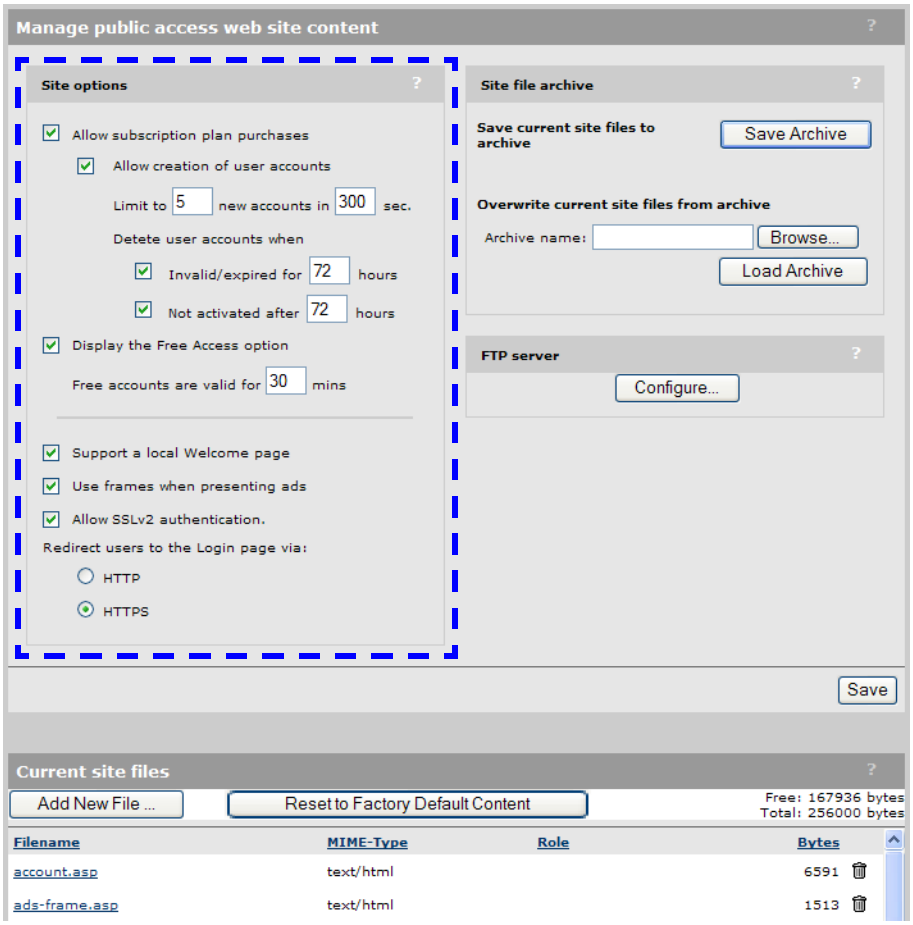
Customizing error messages

To customize the error messages, edit the appropriate messages in the files listed in the following table, using the **Service Controller >> Public access > Web content** page**.**

If an error occurs on	Messages are taken from
Login page (index.asp)	login_error_message.asp
Subscription page (subscribe.asp), Account page (account.asp), Payment page (payment.asp), Review page (review.asp), Purchase failed page (purchase_failed.asp)	subscription_error_message.asp
Other pages (Some errors may result in the user being redirected to the Fail page. This should not occur under normal operation, and will generally only be seen due to a site configuration error. For example, if the URL for a new page is badly configured and the page cannot be found.)	Messages.txt

Setting site configuration options

To view, edit, and manage site options, select **Service controller >> Public access > Web content** and configure the settings under **Site options**.



About ASP variables

A number of ASP variables are defined for use by the public access interface pages. These variables are used to make configuration and status information available via ASP function calls, allowing for customization of the Web pages. Some of the site configuration options set the values of these variables. See *Public access interface ASP functions and variables on page 9-70*.

Allow subscription plan purchases

When enabled, the **Subscribe to this service** option is displayed on the default Login page (index.asp). This option provides a link to the default Subscription page (subscribe.asp), where users can choose one of the subscription plans defined on the **Users > Subscription plans** page. Existing users must enter their username and password to update their current account. New users enter a username and password to create a new account.

For a walkthrough of the public access interface pages related to this option, see *About the "Subscribe to the service" feature on page 8-5*.

Pre-requisites

To use this feature, the following items must be pre-configured:

- One or more subscription plans must be defined by selecting **Users > Subscription plans**.
- To support *credit card* payments, the credit card payment service must be enabled and configured by selecting **Public access > Payment services**.

Display the Free Access option

When enabled, the Free Access option is displayed on the default Login page (index.asp). This enables users to login to the public access interface without paying.

A user account is automatically created for each user that selects the Free Access option. Each account has the following properties:

- The account name and password are set to the MAC address of the user's device.
- The account is valid for up to 30 minutes from the time it is created. To change this time use the **Free accounts are valid for *nn* minutes** option. When a Free Access account expires, the user can choose Free Access again and continue browsing.
- Account settings are imported from the **Default AC** profile. See *About the Default AC profile on page 7-6*.

Free accounts are valid for *nn* minutes

Specify how many minutes a free account is valid, starting from the time the user logs in with the Free Access option.

Support a local Welcome page

Use this feature to host the Welcome page on the service controller Web server.

- When enabled, users are redirected to **welcome.asp** on the service controller Web server.
- When disabled, you can use the welcome-url attribute (see *Default user URLs on page 9-52*) to define a remotely hosted welcome page.

Use frames when presenting ads

This option controls how advertising is displayed:

- When this option is enabled, users are redirected to **ads-frameset.asp**.
- When this option is disabled, users are redirected to **ads.asp**.

For more information on how advertising works, see *Display advertisements on page 8-32*.

Allow SSLv2 authentication

Enable this option to support client stations that use SSL v2 for their HTTPS connections. When disabled, the service controller only supports client stations that are using SSL v3 for HTTPS connections. SSL v2 clients are refused.

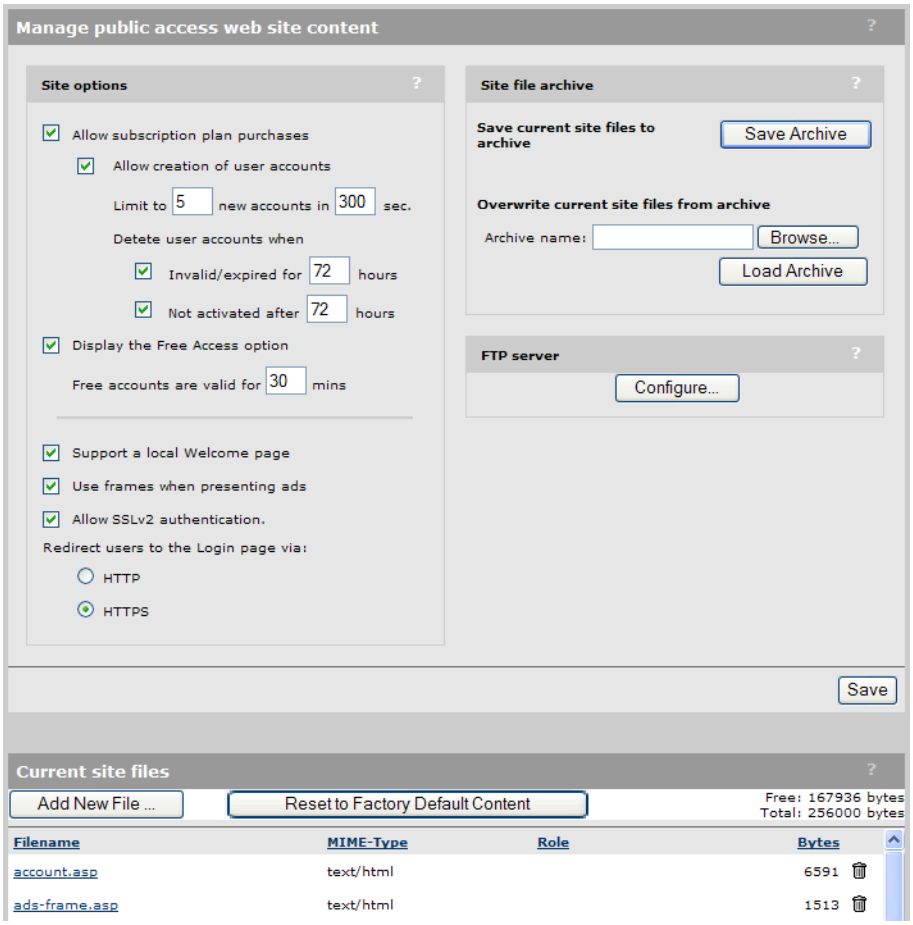
Redirect users to the Login page via

Select the protocol that will be used when redirecting users to the default Login page (index.asp).

- **HTTP:** This option does not provide any encryption for protecting user login credentials.
- **HTTPS:** Provides a secure connection to protect user login credentials. However, until the default SSL certificate that is installed on the service controller is replaced with a certificate signed by a well-known certificate authority, users will see a certificate warning message each time they attempt to log in. See *Managing certificates on page 5-6* for more information on replacing the SSL certificate.

Customizing public access interface Web pages

To view, edit, and customize the public access interface Web page, select **Service controller >> Public access > Web content**.



Site file archive

Use these options to manage the files on the Web server as a single archive file (zip format).

Save current site files to archive

Saves all the current site files to an archive file.

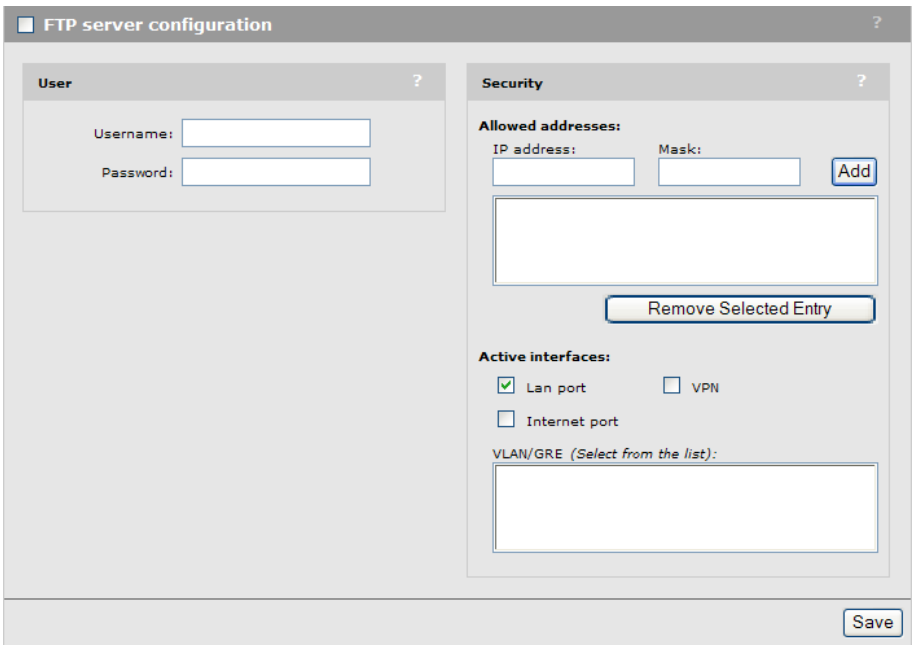
Overwrite current site files from archive

Click **Load Archive** to load all the site files from an archive, overwriting the currently installed site files.

FTP server

The FTP server provides an easy way to manage the public access interface files on the Web server, allowing you to use third-party Web site editing tools to customize content.

Click **Configure** to its define operational settings.



Note For security reasons you should disable the FTP server once the service controller is deployed. Or at minimum, define security filters to restrict FTP access.

User

Specify the username and password that will be required when connecting to the FTP server.

Note When using FTP, the username and password are not encrypted. They are sent as clear text.

Security

Allowed addresses
Enables you to define a list of IP address from which to permit access to the FTP server. To add an entry, specify the IP address and appropriate mask and click **Add**.

When the list is empty, access is permitted from any IP address.

Active interfaces
Select the interfaces through which client stations can access the FTP server.

To select multiple entries, hold down the shift or control key as you click each entry.

Current site files

These are the files that are currently installed on the Web server and make up the public access interface. You can edit and create text files using the built-in editor. Other files must be created offline and uploaded via FTP.

For an overview of the default site structure and control flow, see *Public access interface flow on page 8-11*.

Add New File

Click this button to create a new text-based file on the server.

Reset to Factory Default Content

Click this button to reset the site files to factory default content. You should make a backup copy of the current content using the **Site file archive** options before restoring factory defaults.

About ASP variables

A number of ASP variables are defined for use by the public access interface pages. These variables are used to make configuration and status information available via ASP function calls, allowing for customization of Web page content. Some of the site configuration options set the values of these variables. See *Public access interface ASP functions and variables on page 9-70*.

Site file descriptions

account.asp

text/html

This page is launched by **subscribe.asp** when the user clicks **Next**. It displays a summary of the subscription plan that was chosen and prompts for a username and password to create a new user account.

Clicking **Cancel** launches **index.asp**.

Clicking **Next** launches **payment.asp**.

ads-frame.asp

text/html

This file contains the frame content for ads when using **ads-frameset.asp**.

ads-frameset.asp

text/html

Page that is used to display advertisements using frames. Users see the ad in a frame and their original Web site in second frame.

Users can click the **Continue Browsing** button to return to their original Web page, or continue browsing within the frame.

ads.asp

text/html

Page that is used to display advertisements without frames. Users are redirected to this page while browsing and must click the **Continue Browsing** button to return to their original Web page.

ads.jpg

image/jpeg

This is the default advertisement that is displayed.

fail.asp

text/html

This is a generic error reporting page that is called by various other pages to present an error message.

goodbye.asp

text/html

When a user logs out (by clicking the **Logout** button on the **session.asp** page, for example), if no **goodbye-url** attribute is defined (which specifies the location of a goodbye page), the user is redirected to this page. If this page is missing, than **fail.asp** is presented.

graceful_ending.js

application/javascript

Provides a graceful ending to subscription plans that are about to expire. When a subscription plan has only 10 minutes left or reaches 80% of its transfer quota (these limits are configurable in this script), a warning appears encouraging the user to purchase another plan before their existing one expires.

index.asp

text/html

This is the Login page that users see when they are first redirected to the public access interface.

The Login page contains a single graphic element suitable for a logo or other identifying element and two fields (username and password) that enable users with an existing account to log in. Additional choices may be visible on the Login page if the following features are enabled on the **Service controller >> Public access > Web conten**t page under **Site options:**

- Allow subscription plan purchases
- Display the Free Access option.

login_error_message.asp

text/html

Error messages and the code that is used to display them. Used by **index.asp**.

logo.gif

image/gif

Re-usable image shared by a number of pages.

payment.asp

text/html

This page is called by **account.asp** when a user clicks **Next**.

It displays a summary of the user's subscription selection.

For Authorize.Net payment service:

- Credit card information is requested.
- Clicking **Review**, launches **review.asp.**
- Errors in payment information cause this page to be redisplayed.
- Clicking **Cancel** returns the user to the Login page (index.asp).

For WorldPay payment service:

- Clicking **Go to WorldPay** launches the payment processing page on the WorldPay site.
- Clicking **Cancel** returns the user to the Login page (index.asp).
- See also *WorldPay-cancel.asp/ WorldPay-error.asp/ WorldPay-success.asp on page 8-28*.

prototype.js

application/javascript

Javascript library used to support AJAX for use in **session_ajax.asp** and **subscription_details.asp**.

public-ip.asp

text/html

Message page that is displayed explaining the steps a user must follow to activate a public IP address. This page is only displayed if a public IP address is assigned in the user's account or account profile.

purchase_approved.asp

text/html

This page is displayed as soon as payment is approved.

purchase_failed.asp

text/html

This page is displayed if payment fails.

redirect.asp

text/html

This is the page that is sent when the service controller intercepts a connection from a non-authenticated user. Its function is to redirect the browser to the Login page.

review.asp

text/html

This page is called by **payment.asp** and applies to Authorize.Net payments only.

It displays a summary of the user's subscription selections and presents a **Pay** button. Clicking Pay completes the Authorize.Net transaction. If the transaction is approved, **purchase_success.asp** page is called, otherwise, **purchase_failed.asp** is called.

session.asp

text/html

This page shows usage statistics for the session, as well as the logout button that the user clicks to terminate the session.

session.js

application/javascript

Included by **session.asp.** Provides smart updates for Javascript-based browsers.

session_ajax.asp

text/html

This page is specially designed for AJAX, and provides a JSON page format for use by **session.js** to provide the same content as **session.asp** but for Javascript-enabled browsers. This enables smart refresh of the session data; only changed data is updated, not the entire page, eliminating screen flickering.

Session.asp includes **session.js** which calls **session_ajax.asp**.

sessionwindow.js

application/javascript

Contains Javascript functions used to control opening and closing of the session page.

setfocus.js

application/javascript

Contains Javascript functions used to set the focus to the first form on a page.

style.css

text/css

Stylesheet for all public access interface Web pages.

subscribe.asp

text/html

This page is called by **index.asp** and **session.asp** if **Allow subscription plan purchases** is enabled on the **Service Controller >> Public access > Web content** page under **Site options**.

The page displays all defined subscription plans so that the user can choose one.

The user can click **Next** to proceed to **account.asp**, or **Cancel** in which case they are redirected to **index.asp**.

subscription_details.asp

text/html

This page is called by **session.asp**. it provides information on the subscription plan selected by a user, as well as running totals for data transfer and online time.

subscription_details.js

application/javascript

Included by **subscription_details.asp**. Provides smart updates for Javascript-based browsers.

subscription_details_ajax.asp

text/html

Included by **subscription_details.asp**. Provides smart updates for Javascript-based browsers.

This page is specially designed for AJAX, and provides a JSON page format for use by **subscription_details.js** to provide the same content as subscription_details.asp but for Javascript-enabled browsers. This enables smart refresh of the data; only changed data is updated, not the entire page, eliminating screen flickering.

subscription_details.asp includes **subscription_details.js** which calls **subscription_details _ajax.asp**. Also, **session.asp** includes **gracefulending.js** which calls **subscription_details_ajax.asp**.

subscription_details_window.js

application/javascript

Included by **session.asp**. Contains Javascript functions used to control opening and closing of the subscription details page.

subscription_error_message.asp

text/html

Error messages and code to display them. Used by: **subscribe.asp**, **account.asp**, **payment.asp**, **review.asp**, and **purchase_failed.asp**.

transport.asp

text/html

This page appears briefly after the login is approved and redirects the user to the local or external welcome page.

utils.js

application/javascript

Contains Javascript utility functions used by various public access pages.

welcome-back.asp

text/html

If the **Automatically reauthenticate HTML-based users for *nnn* minutes** option is enabled on the **Service Controller >> Public access > Access control** page under **User authentication**, this page is displayed for returning users instead of the Login page (index.asp).

welcome.asp

text/html

This page is called after the login process is complete if **Support a local Welcome page** is enabled on the **Service Controller >> Public access > Web content** page under **Site options**.

WorldPay-cancel.asp/ WorldPay-error.asp/ WorldPay-success.asp

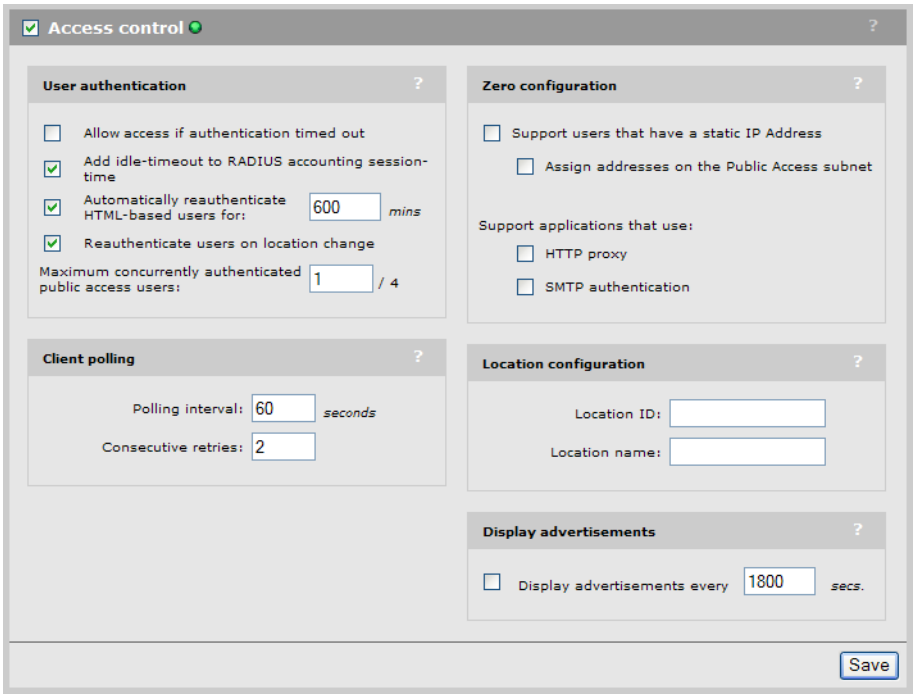
text/html

These pages are retrieved by the WorldPay service during the payment process. This means that the Web server must be accessible to the WorldPay server. Generally this is done by assigning a public IP address to the Internet port. Modifications to these pages must follow WorldPay guidelines.

Global access control settings

The access control mechanism enables the service controller to manage user access to the protected network resources. The features provided by the access control mechanism are only supported on VSCs that are configured for access control.

Support for access control must be enabled and disabled individually for each VSC. Select **Public access > Access control** to configure global settings.



When a VSC is **access controlled**, the options on this page take effect with regards to client station authentication and authorization.

Use the checkbox in the title bar to enable or disable the access control mechanism:

- When enabled, the service controller provides access control which can then be configured on a per-VSC basis to control user logins.
- When disabled, access to the public access interface is disabled for all VSCs that are configured to use access control. Users will not be able to log in using these VSCs.

The status light icon indicates the state of the authentication system.

- A green light icon means that the access control feature is working and authentication requests can be processed.
- A red light icon indicates that access control function cannot process requests at this time.

Access control parameter definitions

User authentication

These settings apply to VSCs that have access control enabled.

Allow access if authentication timed out
Enable this option to give users free access to the public access network if authentication services configured for a VSC are unavailable. Once the authentication service is available again, free user sessions remain active until the user logs out.

For example, if a user is connected to a VSC configured for HTML-based authentication using a RADIUS server, and the RADIUS server is down, the user will be granted free access to the network using the settings from the default user profile.

Note This feature does not work with client stations configured to use 802.1X or WPA.

Add idle-timeout to RADIUS accounting session-time
When enabled, the service controller includes the idle time-out in the total session time for a user when reporting to a RADIUS server. To remove the idle time-out from the total session time, disable this option.

Automatically reauthenticate HTML-based users for up to
When this option is enabled, you can specify the amount of time that the service controller will remember the login credentials for an HTML-based user after they log out. If the user reconnects to the network before this timeout expires, they are automatically logged in, and instead of being redirected to the Login page, they are redirect to the Welcome-back page.

For this feature to work, users must have successfully been logged in at least once via HTML and must have the same IP address and MAC address as their initial login.

To support this functionality, the DHCP server on the service controller will attempt to reserve assigned DCHP addresses even after their lease time has expired. As long as free addresses remain in the DHCP address pool, the expired address will not be reassigned to a new user.

Note The service controller remembers login credentials even if restarted for administrative reasons.

Reauthenticate users on location change
When this option is enabled, the service controller will automatically reauthenticate users when they switch to:

- a wireless cell with a different SSID
- a different VLAN ID on the same VSC
- an AP with a different MAC address
- an AP with a different group name
- a different wireless mode.

Note Location change is not supported for locally authenticated users.

Maximum concurrently authenticated public access users
Specify the maximum number of users that can be authenticated and logged into the public access interface at the same time.

Client polling

The service controller continually polls authenticated client stations to ensure that they are active. If no response is received and the number of specified retries is reached, the client station is disconnected. To use this feature, client stations must have L2 connectivity to the service controller.

This feature enables the service controller to detect if two client stations are using the same IP address but have different MAC addresses. If this occurs, access is terminated for this IP address removing both stations from the network.

Changing these values may have security implications. A large interval provides a greater opportunity for a session to be hijacked.

The initial query is always done after the client station has been idle for 60 seconds. If there is no answer to this query, the settings for **Interval** and **Retries** are used to control additional retries.

Polling interval
Specify how long to wait between polls.

Consecutive retries
Specify how many consecutive polls to which a client station can fail to reply before it is disconnected.

Zero configuration

These settings apply to client stations that are authenticated by the service controller for VSCs that have access control enabled.

Support users that have a static IP address
Enable this option to allow client stations with static IP addresses that are not on the same subnet as the service controller to connect to the service controller. This permits users to access the network without reconfiguring their network settings.

For example, by default the service controller creates a network on the subnet 192.168.1.0. A client station that is preconfigured with the address 10.10.4.99 can connect to the service controller without changing addresses.

- **Assign addresses on the Public Access subnet**: Enable this option to provide network address translation for client stations with static IP addresses. This permits the service controller to assign an alias address to the client station that puts it on the same subnet as the VSC the client station is associated with. This subnet is defined by configuring the DHCP server option in the VSC.

Note This option cannot be used if NAT is enabled on the Internet port.

Support applications that use

- **HTTP proxy:** Enable this option to allow the service controller to support client stations that use a proxy server for HTTP and HTTPS, without reconfiguration of the client stations.

  Ensure that client stations:

  - Do not use a proxy server on ports 21, 23, 25, 110, 443, 8080, or 8090. To support ports 8080 and 8090, change the port settings under **Public access > Web server > Ports**.
  - Use the same proxy server address and port number for both HTTP and HTTPS.

- **SMTP authentication:** When the service controller redirects user SMTP traffic, the server to which the traffic is redirected may need to authenticate the service controller. Enable this option to allow the service controller to supply a username and password to the server. You can define the username and password in the RADIUS account for the service controller or for the user.

Location configuration

These values are returned to IPass clients as well sent in RADIUS authentication Access Requests and Accounting Requests for all users authenticated by this service controller.

Location ID
Specify the WISPr location ID assigned to the service controller.

Location name
Specify the WISPr location name assigned to the service controller.

Display advertisements

When this option is enabled, it causes users to be redirected to an ad content page while they are browsing.

The ads page can be either **ads.asp** or **ads-frameset.asp**, depending on the setting of **Use frames when presenting ads** under **Site options** on the **Public access > Web content** page.

Redirection occurs on TCP port 80.

Note

- Ad display can be suppressed on a per-user basis by setting the appropriate option in the user's account.
- Enabling this feature can cause problems for user applications that expect to obtain network access directly after logging in, instead of being redirected to an ad page.

Display advertisements every *nnn* sec
Specify the interval at which users are redirected to the ads page.

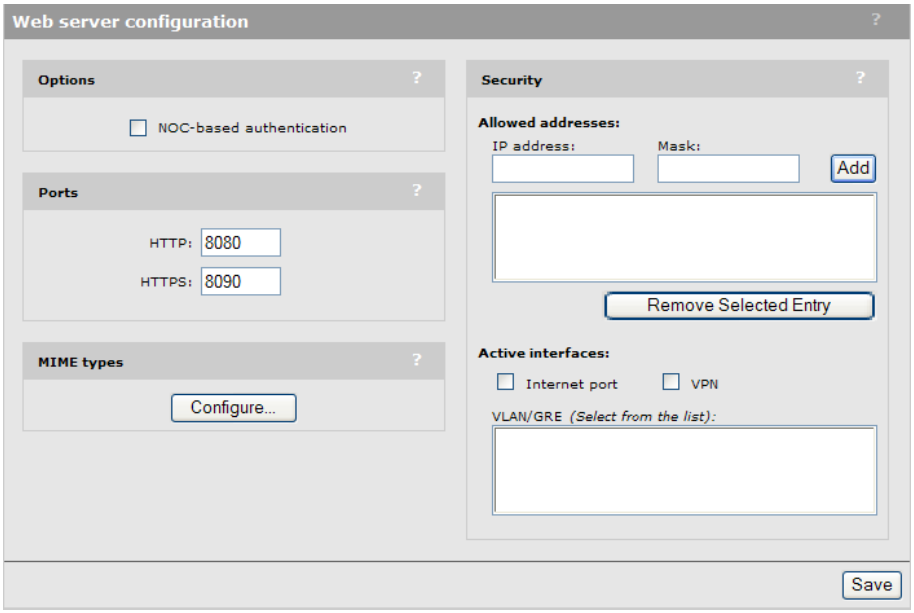
When **Public access > Access control > Advertising** is enabled, users can be redirected to an advertising page at predefined intervals while they are browsing.

Redirection can be controlled by settings in the users account profile, subscription plan, or via RADIUS attributes.

Web server configuration

The service controller features an integrated Web server that, by default, is used to host the Web pages that make up the public access interface. Public access Web pages can also be hosted on third-party Web servers.

Web server configuration settings are defined on the **Public access > Web server** page.



Options

NOC-based authentication
Enable this option to support NOC-based authentication.

NOC-based authentication must be used in conjunction with the remote login page feature. The remote login page feature enables users to be redirected to a remote Web server to log in instead of using the internal login page on the service controller.

To validate user logins, a login application on the remote server must collect user login information and send it to the service controller for authentication.

See also *NOC authentication on page 9-59* and *Appendix D: NOC authentication*.

Ports

Specify the port number the Web server uses for each protocol.

If you enable support for proxy settings under **Public access > Access control > Zero configuration,** you must change the selected port to support client stations that are using proxy servers on the standard port (8080 or 8090). The following mappings are recommended:

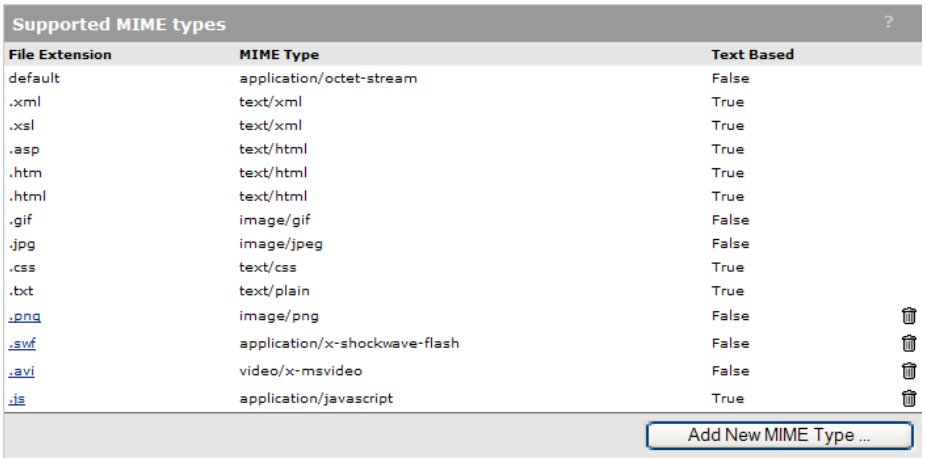
- Map the unsecure port 8080 to port 81
- Map the secure port 8090 to port 444

Make sure that you do not remap these ports to values already in use on your network.

MIME types

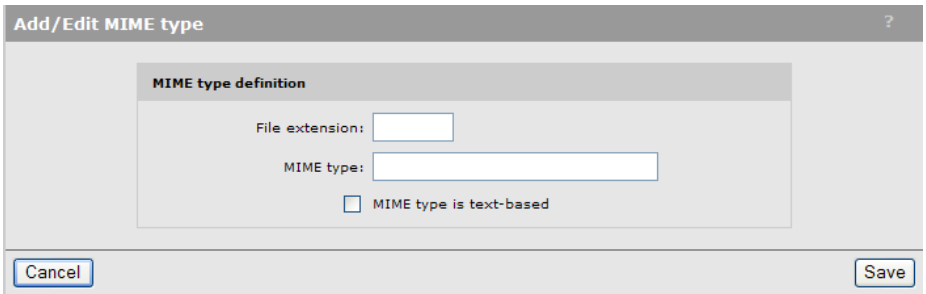
MIME (Multipurpose Internet Mail Extensions) is an Internet standard that is used to describe the type of information that a message or file contains.

By default, the service controller contains the definitions for a number of common MIME types. If you need to add your own definition, click **Configure**.



This page lists all MIME types that are currently defined on the Web server. A number of common MIME types are defined by default. (Some of the default definitions cannot be changed.)

Click **Add New MIME Type** to define your own MIME type.



File extension
Specify the file extension that identifies this MIME type.

MIME type
Specify the content-type string that identifies this MIME-type. This is the value that must appear in an HTTP Content-type header for the service controller to recognize this MIME type.

Types should be specified in the following format: **type/subtype**

For example: **text/xml**

MIME type is text-based
Enable this option if the MIME type identifies files that are text-based.

Security

Use this option to control access to the Web server.

Allowed addresses
The Web server will only accept connections from devices whose IP addresses appear in this list.

When the list is empty, authentication requests are accepted from any address.

Active interfaces
Select the interface(s) on which the service controller will accept connections.

When NOC authentication is active, this is the interface on which the remote login Web server application can be reached. For more information on NOC authentication, see *NOC authentication on page 9-59* and *Appendix D: NOC authentication*.

Note

Ingress interfaces configured inside VSCs (including the LAN port) always have access to the Web server when NOC-based authentication is disabled.

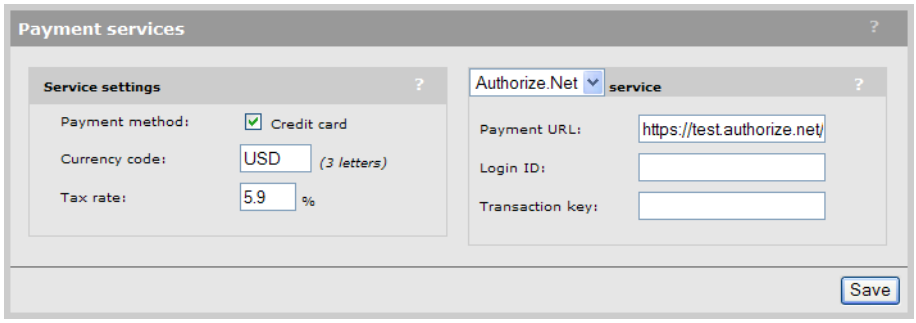
Payment services

The service controller can directly interact with payment processing services service such as Authorize.Net and WorldPay, so that users can pay for network access from within their Web browser.

Payment services configuration

To configure payment services, follow this procedure:

1. Select **Service Controller >> Public access > Payment services**.



   Use this page to define the type of payment options that the public access interface will support

2. Enable **Credit card**. Specify the 3-letter **Currency code** (see online help for list of codes) and **Tax rate**.

3. For Credit card payment authorization, select either Authorize.NET or WorldPay, and specify the appropriate information. Merchant accounts must be set up to use these services (www.authorize.net or www.worldpay.com).

Service settings

Payment method: Credit card
Enable this option to allow users to pay for services via credit card. The service controller makes use of a third-party credit card processing service (either Authorize.Net or WorldPay) to handle credit card transactions.

Communications with the credit card service occurs via an SSL connection that is secured using a digital certificate. This certificate is not supplied. You must purchase the appropriate certificate as required by the credit card service provider and install it on the **Service controller >> Security > Certificates stores** page.

The service controller does not keep a record of the user's credit card information. All information handled by the system is securely managed in accordance with the PCI DSS v1.2 standard.

The service controller maintains a billing log that provides a simple audit trail of all transactions The log supports the buffering and retransmission of up to 2000 billing records to an external billing records server. You can configure log options on the **Service controller >> Public access > Records** page.

Currency code
Specify the three-letter code for the currency in which all charges will be calculated. See the online help for a complete list of currency codes.

Tax rate
Specify the tax rate to use when calculating sales tax for all charges.

Authorize.Net service

Payment URL
Specify the URL of the Authorize.Net server.

Login ID
Specify the login ID of the Authorize.Net account assigned to the service controller.

Transaction key
Specify the transaction key for the Authorize.Net account assigned to the service controller.

WorldPay service

Payment URL
Specify the URL of the WorldPay server.

Installation ID
Specify your WorldPay installation ID. This informs WorldPay to which merchant all sales will be credited.

Response password
Specify your WorldPay installation response password.

Other configuration issues
To successfully make use of the WorldPay service you must also address the following issues:

- The Internet port of the service controller must be reachable by the WorldPay servers. This is required so that the WorldPay pages stored on the service controller can be retrieved, and that the service controller can receive an HTTP/HTTPS post with payment details. (To support HTTPS, a certificate signed by a well-known certificate authority must be installed on the service controller.)
- An access list must be defined on the service controller that gives users access to the WorldPay site without being authenticated. For example:
  `access-list=factory,ACCEPT,tcp,*worldpay.com,all`

  If different, replace `*worldpay.com` with whatever is configured.

For complete configuration requirements, see the documentation on the WorldPay site.

Billing record logging

The billings records logging system provides a simple audit trail of all billing transactions.

The log supports the buffering and retransmission of up to 2000 billing records to one or more external billing records servers. Log transmission occurs using HTTP/1.1 POST method with a completely customizable data format.

The system will retransmit a billing record until it is successfully acknowledged or until transmission is stopped because of too many failures.

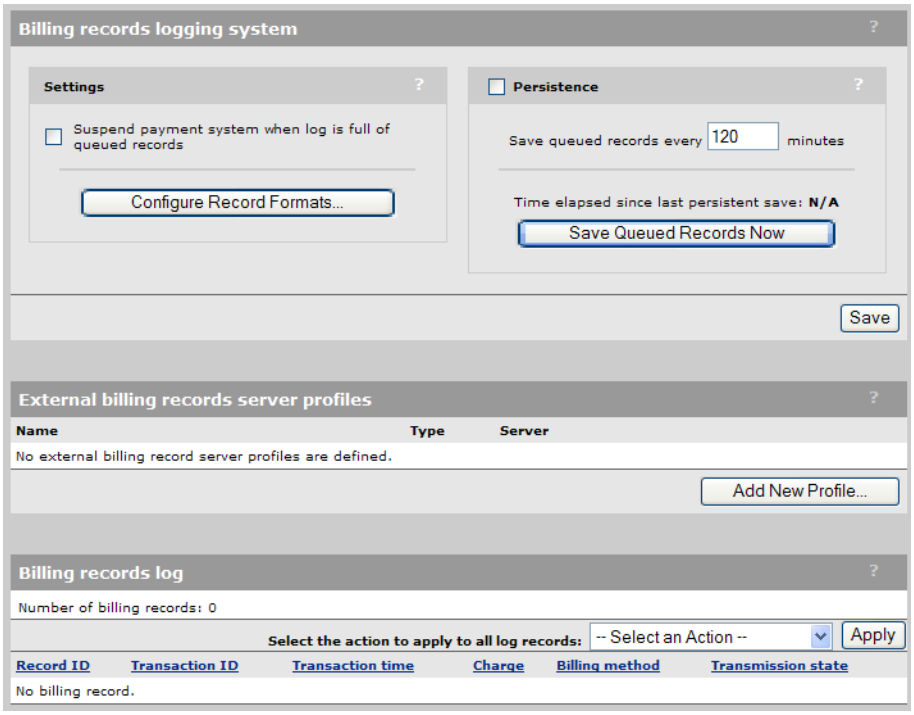
Multiple backup servers can be assigned to a primary server to increase the probability of successfully transmitting a billing record.

To reduce the risk of billing records being lost, data can be mirrored by defining multiple primary servers. A copy of each record is sent to each primary server.

Note

Records are always added to the log, even when record transmission is disabled. If required, these records can be saved (exported) to a file, but cannot be transmitted to a billing server.

To configure Billing record logging, select **Service Controller >> Public access > Billing records**.



Settings

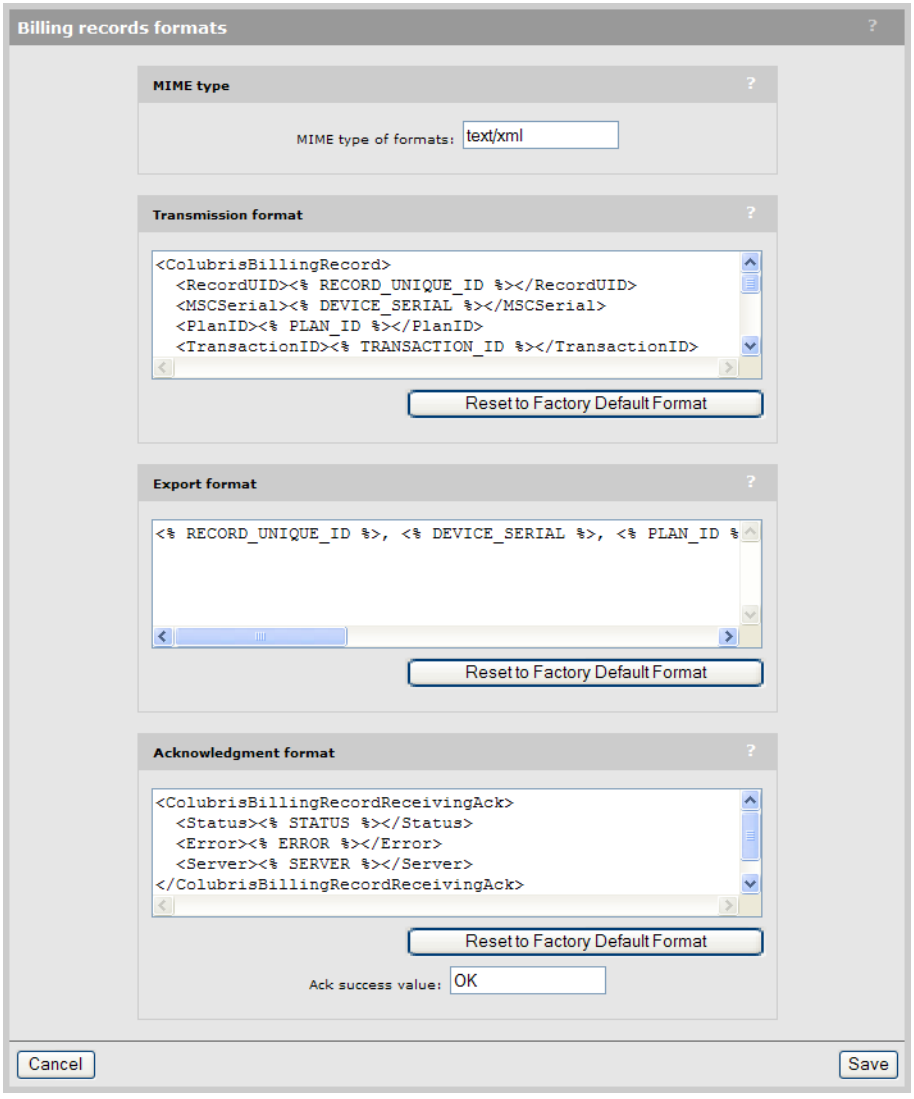
Suspend payment system when log is full of queued records

Use this option to halt the payment system if external billing servers are unable to receive records and the log is full of **untransmitted** records. (Records with a status of "Queued"). For more information on how the log entries are managed, see *Billing records log on page 8-43*.

When this options is disabled, the oldest untransmitted record is removed from the log to make room for the new record.

Configure Record Formats

Click this button to edit the transmission, export, and acknowledgement formats for the billing records. See the online help for format descriptions.



Persistence

Enable this option to have the service controller save queued (untransmitted) records in the log to its internal flash memory so that they can be recovered in case of abnormal system shutdown (power failure, for example). See *Billing records log on page 8-43*.

Save queued records every *nn* minutes
Specify the interval at which the log is saved.

Save Queued Records Now
Force the log to be saved immediately.

External billing records server profiles

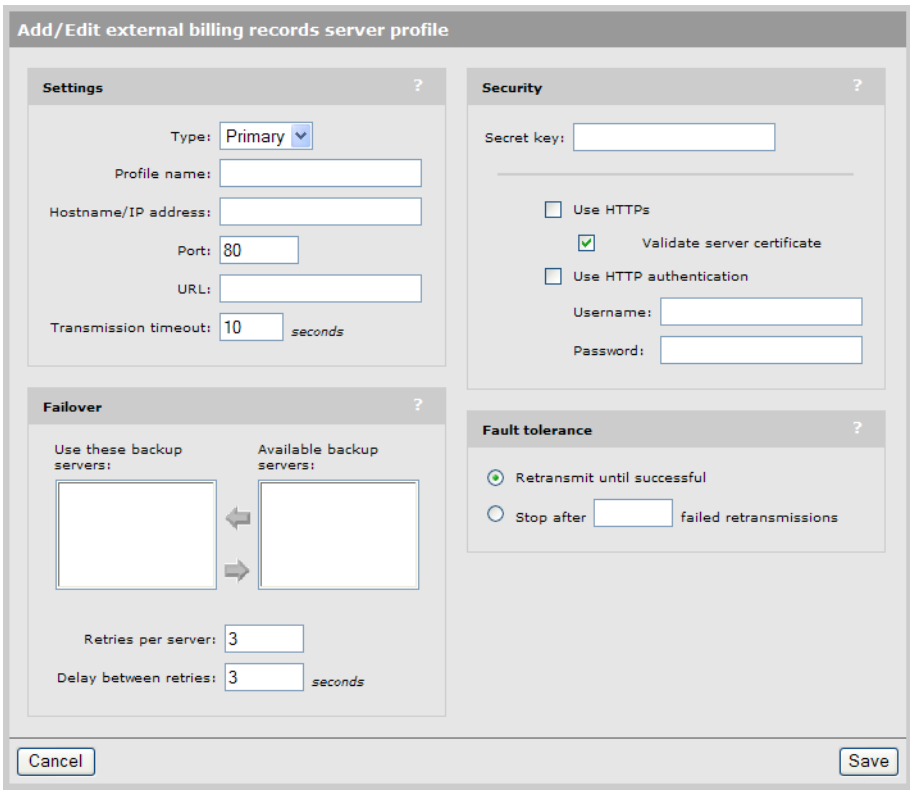
This list displays all configured billing records server profiles. Billing records are sent to the servers defined in this list as follows:

- A copy of the current billing record is sent to each primary server. By adding multiple primary servers you create data mirroring and reduce the risk of a record being lost.
- If a primary server fails to acknowledge the record, the service controller retries. Once the retry limit is reached, the record is transmitted to any defined backup servers. Once all retries are attempted for all backup servers, the record is either skipped, or the entire process starts again.

For example, if you configure a primary server “Server A” with “Server B” as a backup, with 2 transmission attempts, the following sequence in used to transmit the billing record:

A-[Delay]-A-[Delay]-B-[Delay]-B-[Delay]-A-[Delay]-A-[Delay]-B-[Delay]-B…

To edit an existing profile, click its **Name**. To add a new profile, click **Add New Profile**. In either case you will see the Add/Edit external billing records server profile page.



Settings

Type

- **Primary:** Defines a primary server. The service controller sends a copy of each billing record to all primary servers. See *Record transmission overview on page 8-43*.
- **Backup:** Defines a backup server. Backup servers can be assigned to act as a backup to a primary server by using the **Failover** box.

Profile name

Specify a name to identify the server profile.

Hostname/IP address

IP address or hostname of the server.

Port

Port on which to send the HTTP post.

URL

URL to which the HTTP post will be sent.

Transmission timeout

Amount of time that the service controller waits for an HTTP response for a transmitted record. If the response is not received within this period, this is considered as a failed transmission.

Failover

Use this box to define one or more backup server profiles for the current primary server profile.

Use these backup servers
Lists all backup server profiles for this primary server profile. Backup profiles are used in the order that they appear in the list.

Available backup servers
Lists all server profiles of type backup.

Retries per server
Number of times that a record will be retransmitted before the next profile is tried.

Note

This parameter also sets the number of retries on the primary.

Delay between retries
Amount of time to wait between retransmitting a record.

Security

Encryption and authentication can be used to increase the transmission security of billing records.

HTTP authentication and secure HTTP using SSLv3 are supported. Also, to make sure that a billing record has not been altered, a secret key, shared between the billing server and the service controller, can be defined and used to produce a cryptographic signature of the billing record.

Secret key
Specify the secret key that will be used to generate an encryption signature using HMAC-SHA-1. The signature is generated using the entire contents of the billing record. (The signature field is empty when the signature is calculated.)

Use HTTPS
When enabled, secure HTTP using SSLv3 is used to transmit records to all servers.

Validate server certificate
When enabled, the service controller will validate the external billing server certificate. For this to be successful, you must install the billing server CA certificate in the Trusted CA certificate store on the **Security > Certificate stores** page.

Use HTTP authentication
Enable this option if the billing server requires a username and password.

Fault tolerance

Fault tolerance settings control how many times each billing record is retransmitted.

Retransmit until successful
When enabled, the service controller will never skip a record due to transmission failure. Retransmission is continuously retried on the primary server and all backup servers until successful.

Enabling this option may cause log entries to be lost if a record fails to be transmitted before the log wraps around. To avoid losing records, enable the **Suspend operation of payment system when log is full** option under **Log settings** on the **Service controller >> Public access > Billing records** page.

Stop after failed *nnn* retransmissions
Select this option to have the service controller stop retransmitting a record when the total number of retransmissions on all servers (primary and backup) exceeds the specified number.

When this occurs the record is flagged as **Transmission Failed** in the log.

Record transmission overview

Transmission of a billing record occurs as follows:

- Billing record is transmitted to the primary server.
- If the primary server does not send an HTTP reply within the **Transmission timeout**, then the transmission is considered to have failed. If a response is received, but the status field does not match the value of **Ack success value**, then the transmission is considered to have failed.
- Failed transmissions are retried on the primary server until the **Retries per server** limit is met, after which each backup server is tried in order. Once all backups are tried, the sequence resumes again with the primary server.
- Retransmissions only stop if the selected condition under **Fault tolerance** is met: either the record is successfully transmitted or the total number of retires on all servers passes a predetermined limit.

Note

A billing record is considered to be successfully transmitted only when it has been successfully transmitted to **every primary server** (or one of its backups).

Billing records log

This table displays the contents of the billing records log. The log can hold up to 2000 records. When full, records are deleted in the following order:

1. Records that have been successfully transmitted.
2. Records that do not have to be transmitted, because transmission is disabled.
3. Records for which transmission has failed.

If transmissions to remote billing server(s) is interrupted, the log can become full of untransmitted records only. (Records with status set to “Queued”.) What happens next is controlled by the **Suspend payment system when log is full of queued records** when log is full setting under **Settings**.

- If enabled, payment services are suspended.
- If disabled, the oldest queued record is removed.

Number of billing records
Lists the total number of billing records in the log.

Select the action to apply to all log records

- **Clear log:** Delete all records in the log.
- **Save log:** Save the log to a file using the export format defined by selecting **Service controller >> Public access > Billing records > Configure Records Format**.
- **Retransmit failed records:** Force the retransmission of records that have transmission state set to **Transmission Failed**. This starts the complete transmit cycle all over again for the record.
- **Cancel current transmission:** Terminates the record transmission that is currently in progress.

Table

Record ID
Unique number that identifies each record.

Transaction ID
Credit card transaction ID generated by the credit card service.

Transaction time
Date and time of the transaction.

Charge
Amount charged on the transaction.

Billing method
Identifies the billing method:

- CC - WorldPay
- CC - Authorize.Net

Transmission state

- **Transmitting:** The record is being transmitted.
- **Queued:** The record is queued for transmission.
- **Transmission Disabled:** Transmission of the record was disabled. Once records fall into this category they cannot be retransmitted.
- **Successful:** The record was successfully transmitted and acknowledged by all primary servers (or their backups).

- **Transmission Failed:** The record was not transmitted successfully and retransmission attempts have stopped due to the setting for **Fault tolerance** in the billing records server profile (**Service controller >> Public access > Billing records > External billing records server profiles**).

Location-aware authentication

This feature enables you to control logins to the public access network based on the wireless access point with which a user is associated. Once authenticated, this feature is also used to monitor and control roaming to other access points in the network.

How it works

Location-aware is automatically enabled when a VSC is set to **provide access control**. When enabled, the location-aware feature causes the service controller to return location-specific information for RADIUS-authenticated users. This information is returned:

- When the user logs in
- Each time the user roams to a new access point or switches SSIDs on the same access point (which causes the user to be re-authenticated).

Note Due to security constraints in 802.1X client software, users cannot automatically be re-authenticated when roaming to a new access point. Therefore, location-aware information cannot be returned when these users roam.

Returned information

The service controller can return the following attributes in the RADIUS access request for all user authentications (whether initial login or re-authentication due to roaming).

- Called-station-ID (Standard RADIUS attribute)
- ProCurve-specific attribute: SSID
- ProCurve-specific attribute: GROUP.

Note When re-authenticating users, the returned RADIUS attribute Service-Type is set to 8744 (decimal).

Called-Station-ID value

By default, this is the MAC address of the wireless port (radio) the user is associated with. This is the MAC address of the **wvlan0** or **wvlan1** interface in IEEE format as displayed by **Tools > System Tools > Interface info.**

If required, the service controller can return other values for this attribute by setting the **Called-Station-Id content** on a per-VSC basis. The other available options are:

- SSID: SSID of the access point with which the user is associated.
- GROUP: Group name of the access point with which the user is associated.

Note

If the user is connected via a wired connection, the value returned is the MAC address of the service controller wireless/LAN port. To use the MAC address of the Internet port, you must edit the config file and change the setting of **radius-called-station-id-port** to **WAN** in the <ACCESS-CONTROLLER> section.

ProCurve-specific attribute: SSID

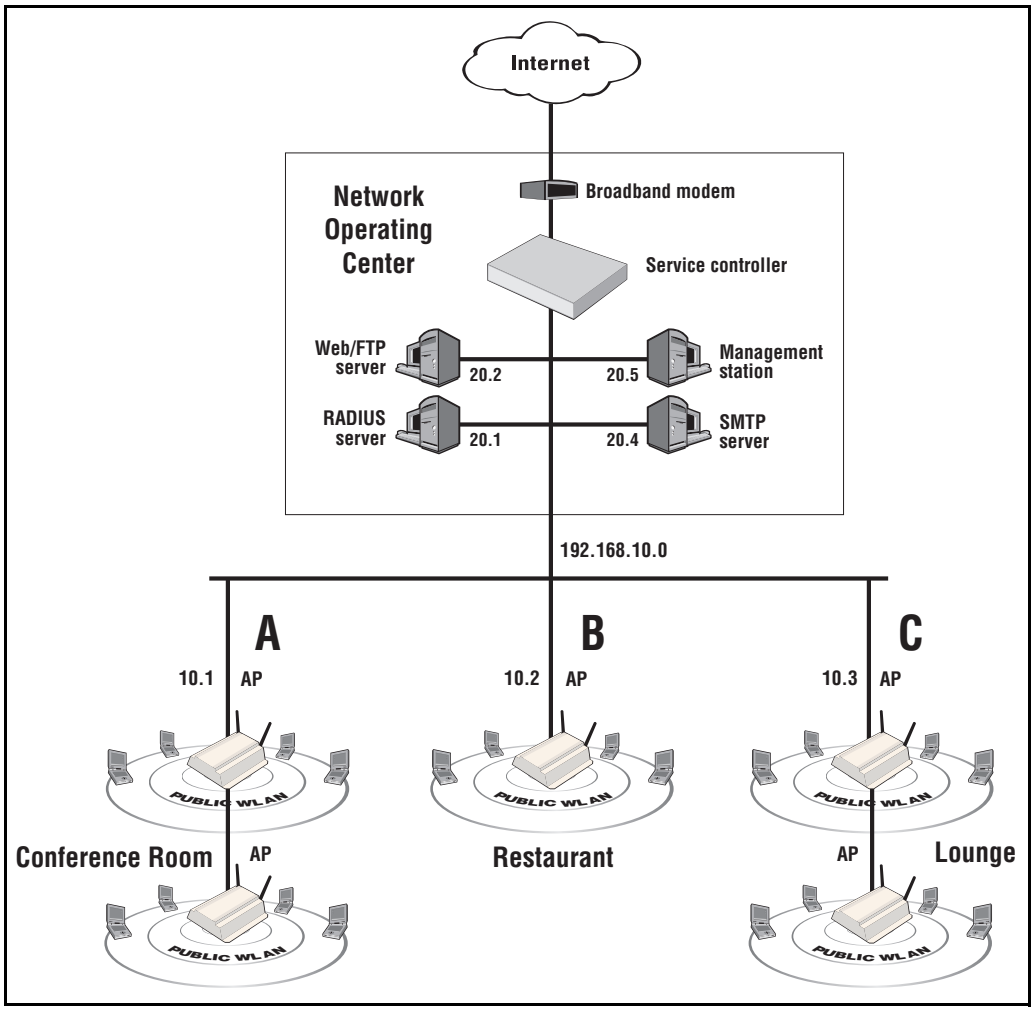
The SSID of the access point with which the user is associated (wireless only).

ProCurve-specific attribute: GROUP

The GROUP of the access point with which the user is associated (wireless only).

Example

Consider the following topology for a fictional small hotel. The restaurant and lounge are available to all hotel users who subscribe to the wireless service. However, the conference room is available only to a specific group of guests who book it in advance.



In this example, the access points in each area are assigned the following unique group names:

- conference_room
- restaurant
- lounge

When a user logs in, server-side code can be used to determine the access point they are associated with by inspecting the Called-Station-ID. Then, using user's account information, access can either be granted or denied.

Security

The service controller accepts location-aware information only from MSM APs that have a matching shared secret to its own.

9

Working with public access attributes

Contents

Defining and retrieving site attributes 9-3
Retrieve attributes using RADIUS 9-3
Configured attributes 9-4

Defining and retrieving user attributes 9-5
Defining attributes locally in user accounts 9-5
Retrieving attributes from a RADIUS server 9-9

Attribute definitions 9-10
Site attributes 9-11
User attributes 9-17
Administrator attributes 9-27

Colubris AV-Pair attribute - Site values 9-29
Access list 9-30
Configuration file 9-41
Custom SSL certificate 9-41
Custom public access interface Web pages 9-42
Default user interim accounting update interval 9-48
Default user bandwidth level 9-49
Default user idle timeout 9-49
Default user quotas 9-49
Default user data rates 9-50
Default user one-to-one NAT 9-50
Default user session timeout 9-51
Default user public IP address 9-51
Default user SMTP server 9-51
Default user URLs 9-52
HTTP proxy upstream 9-52
IPass login URL 9-53

MAC authentication 9-53
Multiple login servers 9-54
Redirect URL 9-56
NOC authentication 9-59
ProCurve WISPr support 9-59
Traffic forwarding (dnat-server) 9-60
Multiple DNAT servers 9-61

Colubris AV-Pair attribute - User values 9-63
Access list 9-64
Advertising 9-65
Bandwidth level 9-65
Data rate 9-65
One-to-one NAT 9-66
Public IP address 9-66
Quotas 9-66
Redirect URL 9-67
SMTP redirection 9-67
Station polling 9-68

Colubris AV-Pair attribute - Administrator values 9-69
Administrative role 9-69

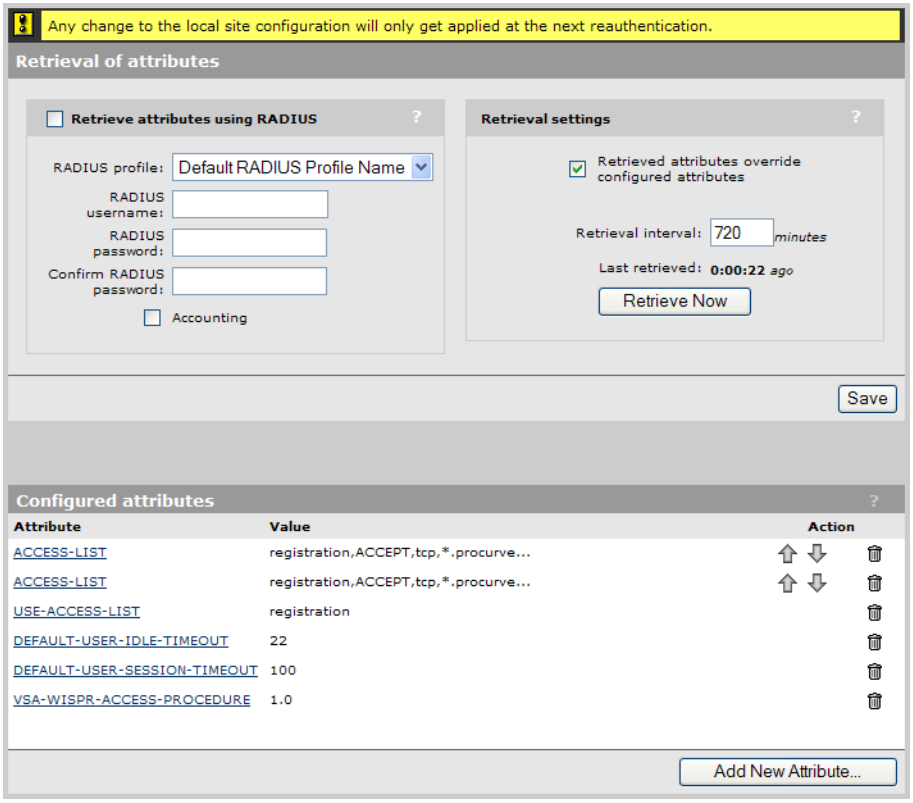
Public access interface ASP functions and variables 9-70
Javascript syntax 9-71
Forms 9-71
Form errors 9-74
RADIUS 9-75
Page URLs 9-76
Session status and properties 9-77
iPass support 9-81
Web 9-83
Client information 9-83
Subscription plan information 9-85
Other 9-86
Session information 9-89

Defining and retrieving site attributes

RADIUS attributes can be used to define a number of features for the public access interface. Attributes can be retrieved from a third-party RADIUS server or defined directly on the service controller.

For a complete list of all supported site attributes, see *Site attributes on page 9-11*.

Select **Public Access > Attributes** to open the **RADIUS Attributes** page.



Configurable parameters on the **RADIUS Attributes** page include those described in the following sections.

Retrieve attributes using RADIUS

If you enable this option, the service controller will use the services of a third-party RADIUS server to retrieve configuration settings for customization of the public access interface. The settings must be defined in a RADIUS account for the service controller.

The retrieved attributes are combined with those defined in the **Configured attributes** list (if any) to build the complete list of defined attributes. If the same attribute is defined on both the RADIUS server and in the **Configured attributes** list, the setting of **Retrieved attributes override configured attributes** determines which setting is used.

Note

The total number of attributes that can be defined via RADIUS and the **Configured attributes** list is 128 attributes.

Enable the **Retrieve attributes using RADIUS** option to configure the following parameters:

- **RADIUS profile**: Select a RADIUS profile. The profile is used to establish the connection to a RADIUS server. RADIUS profiles are defined by selecting **Service controller >> Authentication > RADIUS profiles**.
- **RADIUS username**: Specify the username of the RADIUS account assigned to the service controller.
- **RADIUS password / Confirm password**: Specify the password of the RADIUS account assigned to the service controller.
- **Accounting**: Enable this option to have the service controller generate a RADIUS accounting request ON/OFF each time its authentication state changes.
- **Retrieved attributes override configured attributes**: Enable this option to have attributes retrieved from the RADIUS server overwrite settings defined in the **Configured attributes** table.
- **Retrieval interval**: Specify the number of minutes between attribute retrievals. The service controller retrieves attributes from its RADIUS account each time this interval expires.

  To avoid potential service interruptions that may occur when new attributes are activated by the service controller, it is strongly recommends that you use a large interval (12 hours or more).

  You can override the value configured on this page by using the RADIUS attribute **Session-timeout**, which enables the following strategy: Configure **Retrieval interval** to a small value (10 to 20 minutes) and set the RADIUS attribute **Session-timeout** to override it with a large value (12 hours) when authentication is successful. Since the **Retrieval interval** is also respected for Access Reject packets, this configuration results in a short reauthentication interval in the case of failure, and a long one in the case of success.
- **Last retrieved**: Shows the amount of time that has passed since the service controller last retrieved attributes.
- **Retrieve Now**: Select to force the service controller to contact the RADIUS server and retrieve attributes.

Configured attributes

HP ProCurve has defined a vendor-specific RADIUS attribute to support configuration of the public access interface and user accounts. This attribute conforms to RADIUS RFC 2865 and is called the Colubris AV-Pair.

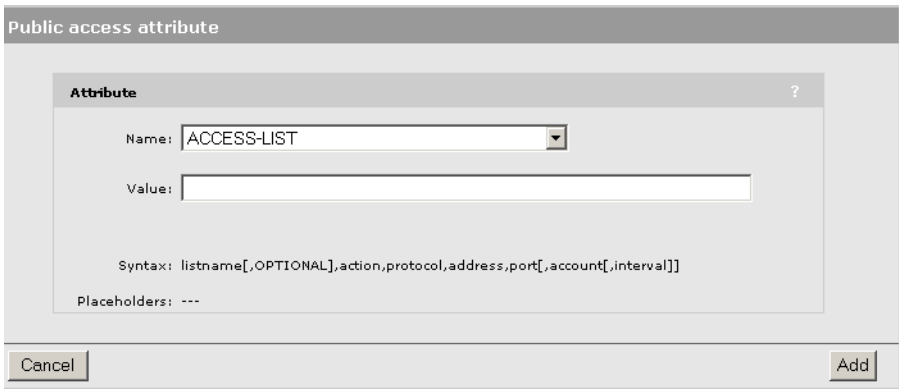
Multiple instances of the Colubris AV-Pair attribute can be defined to configure a variety of settings. Each instance is called an AV-Pair value. This table lists all AV-Pair values that are defined on the service controller.

For a complete list of all supported AV-Pair values, see *Colubris AV-Pair attribute - Site values on page 9-29*.

If you enable the **Retrieve attributes using RADIUS** option, the Colubris AV-Pair attribute values can also be defined in the RADIUS account for the service controller. When the service controller authenticates itself, it retrieves these AV-Pair values. These retrieved values will overwrite the configured attributes in this table if the **Retrieved attributes override configured attributes** option is enabled.

To add a new attribute:

1. Select **Add New Attribute.** The **Public access attribute** page opens.
2. Under **Name,** select an AV-Pair value, as shown in the following figure.



3. Once you select a **Name,** information appears regarding the correct syntax to specify under **Value.** Use the correct syntax to specify the desired **Value**.
4. Select **Add.**

Defining and retrieving user attributes

RADIUS user attributes can be used to define a number of features for user accounts. User attributes can be configured locally in user account profiles, or retrieved from a third-party RADIUS server.

For a complete list of all supported user attributes, see *User attributes on page 9-17*.

Defining attributes locally in user accounts

If you are using the local user accounts to authenticate users, then you can define account attributes locally via account profiles.

Each user account can be associated with one or more account profiles. The attributes that are set in each profile are combined in the account to produce the full list of supported attributes.

If you are working with access-controlled user accounts, additional attributes can also be defined via the **Default AC** profile.

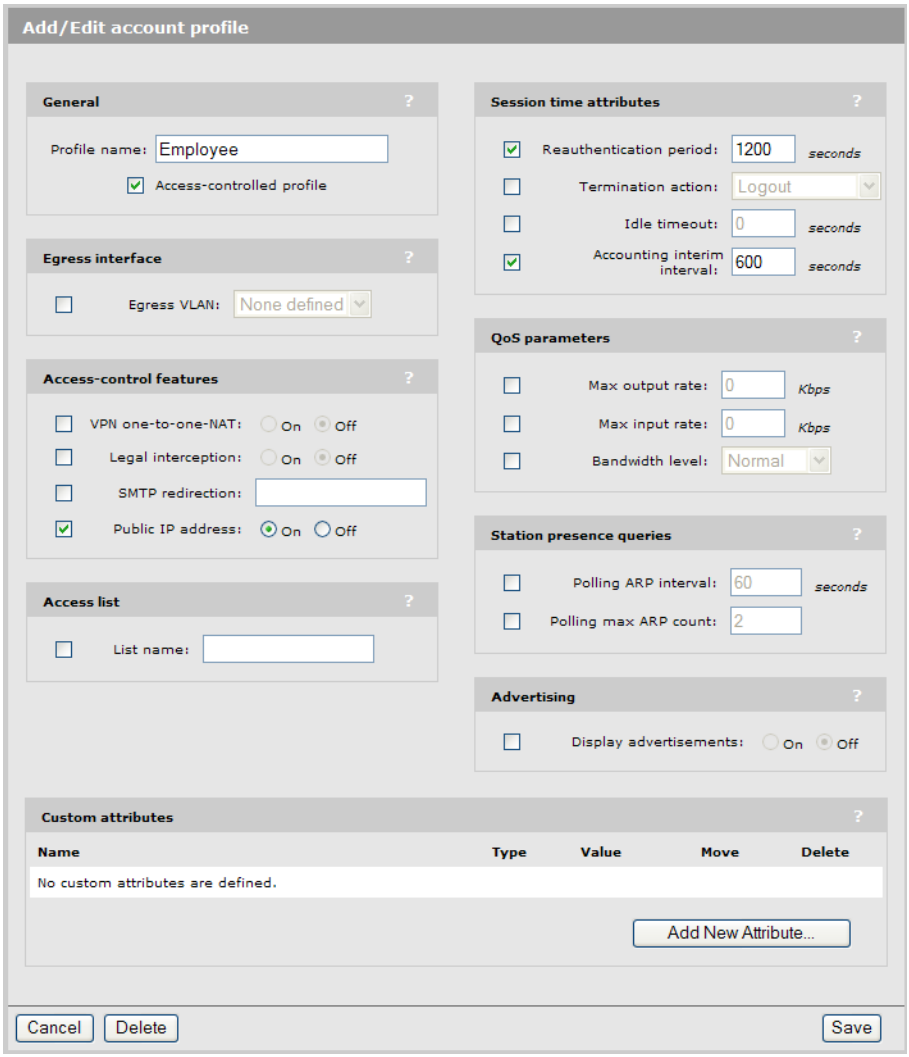
The best way to understand how all this works is to look at an example.

Example

In this example, two user profiles (called **Employee** and **Guest**) are defined on the **Service Controller >> Users > Account profiles** page. The settings for each profile are shown below.

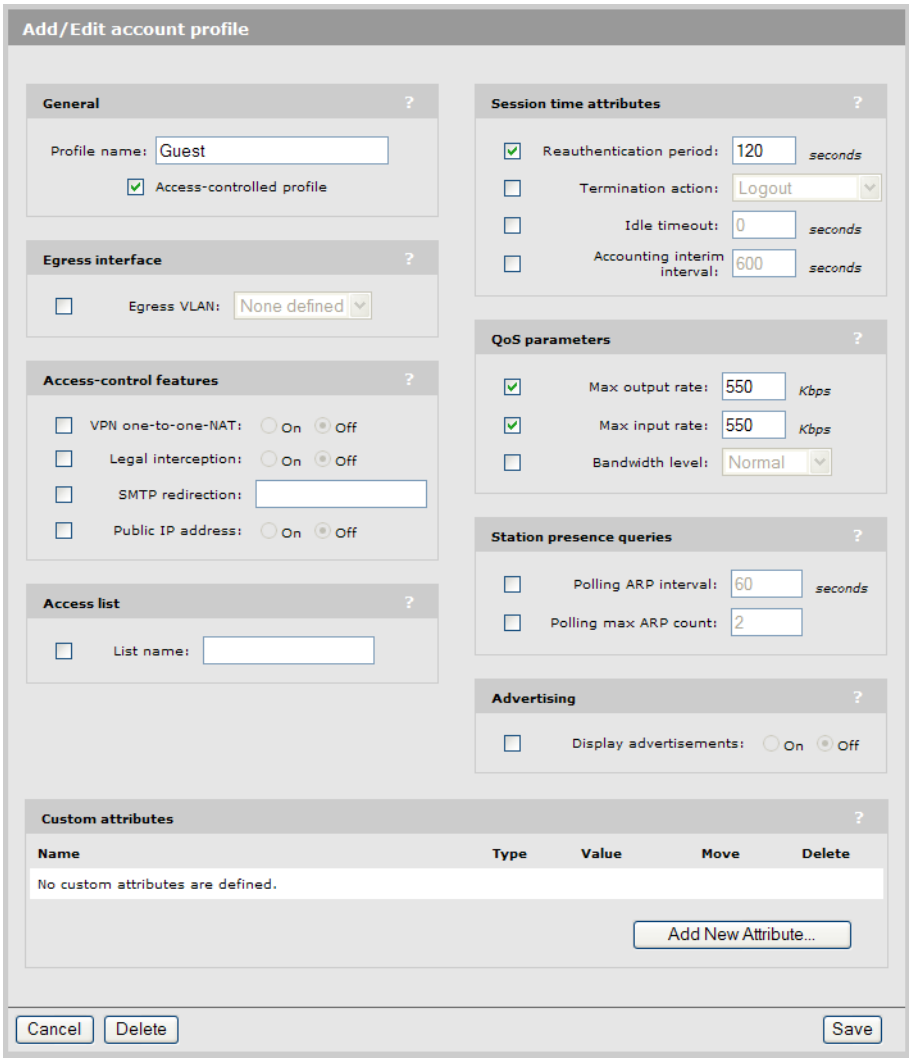
Employee profile

Sets the attributes that will be used to define employee accounts.



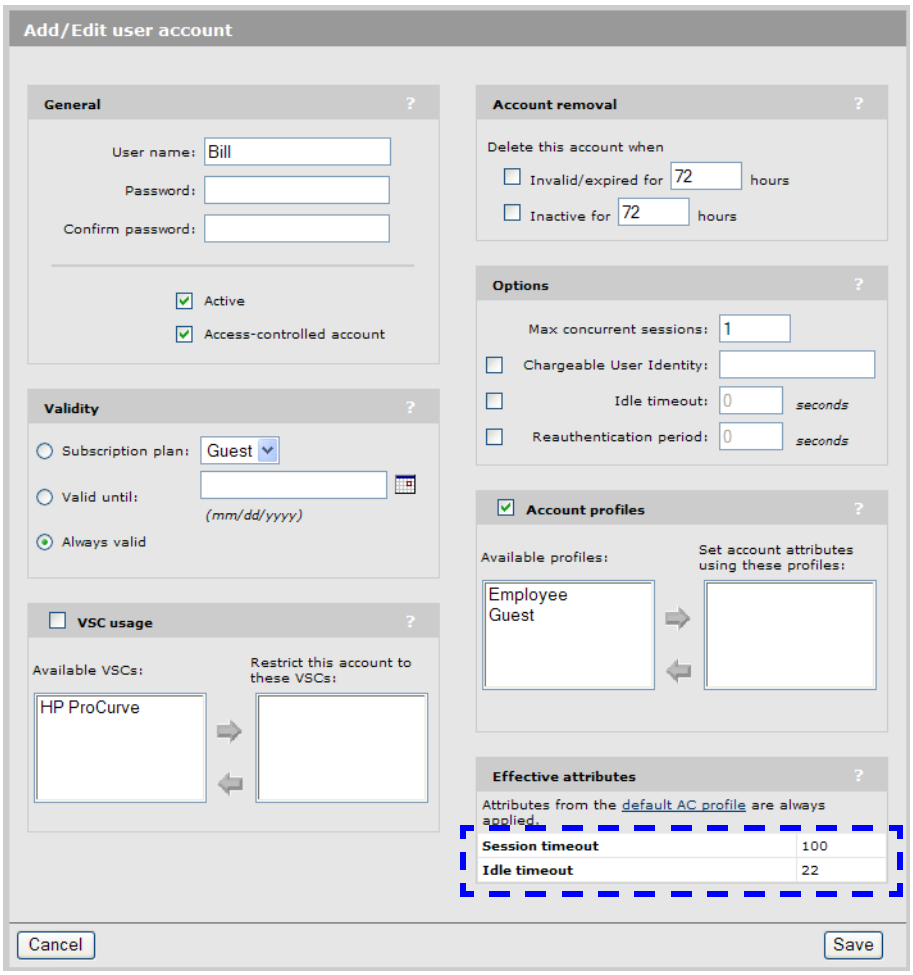
Guest profile

Sets the attributes that will be used to define guest accounts.



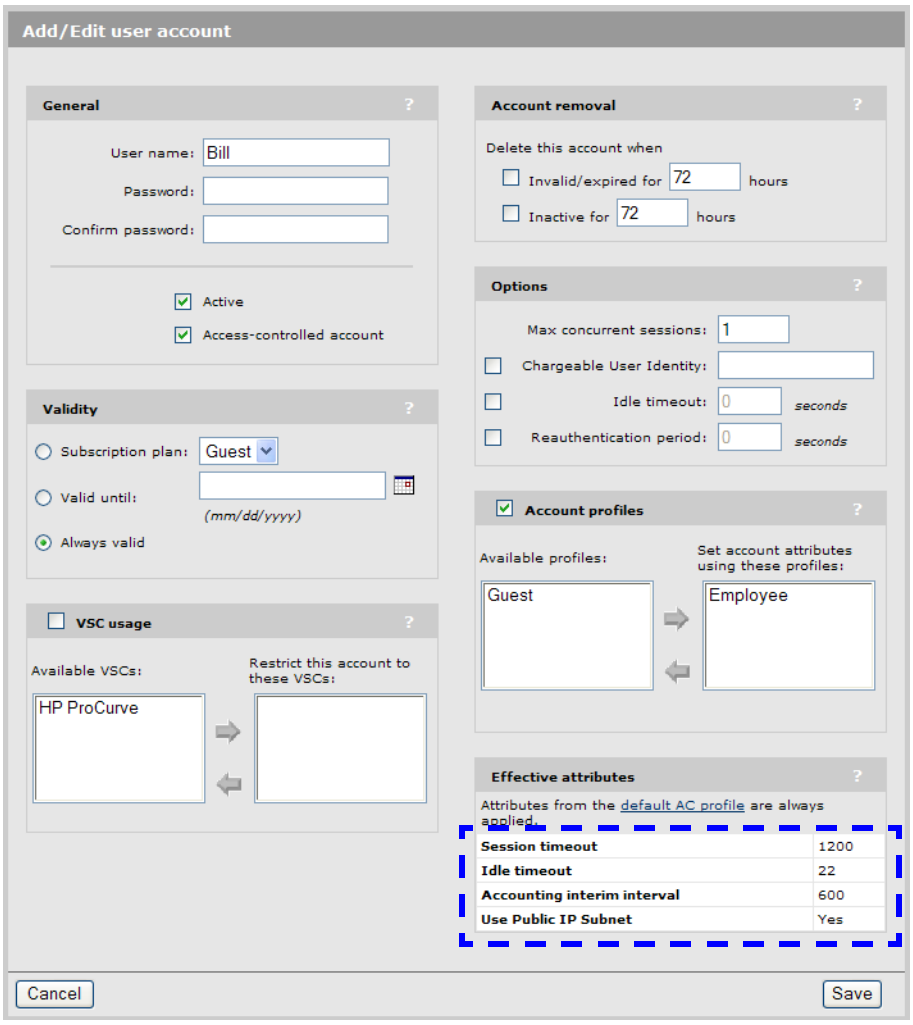
Once account profiles have been defined, user accounts can be created.

The following sample page shows the initial configuration of a user account for an employee named **Bill**. Notice that before any account profile is assigned, the **Effective attributes** box shows a couple of active attributes: **Idle timeout**, and **Session timeout**.



These attributes come from the **Default AC** profile. Attributes from this profile are automatically assigned to all access-controlled user accounts. To customize the attributes for the **Default AC** profile you need to select **Service controller >> Public access > Attributes**. (The default AC profile cannot be edited via the **Service controller >> Users > Account profiles** page.) See *About the Default AC profile on page 7-6*.

To complete the configuration of Bill's account, the **Employee** account profile is assigned, which adds additional attributes to the **Effective attributes** list.



Retrieving attributes from a RADIUS server

When you are using a RADIUS server to authenticate users, attributes can be set in individual user accounts to define the same settings that are available via the local user profiles. For a complete list of all supported attributes and how to define them, see *User attributes on page 9-17*.

Attribute definitions

RADIUS attributes are used to define a number of features for the public access interface. Attributes can be retrieved from a third-party RADIUS server or defined directly on the service controller. Supported RADIUS attributes are divided into two categories:

- *Site attributes on page 9-11*
- *User attributes on page 9-17*
- *Administrator attributes on page 9-27*

The maximum attribute size that the service controller can receive in a single RADIUS request is 4096 bytes. However, some networks may limit RADIUS request size to around 1500 bytes because they discard UDP fragments. In the attribute descriptions, a *string* is defined as 1 to 253 characters.

Site attributes

The following site attributes are supported.

Access Request

- Acct-Session-Id
- Called-Station-Id
- Calling-Station-Id
- CHAP-Challenge
- CHAP-Password
- Connect-Info
- EAP-Message
- Framed-IP-Address
- Framed-MTU
- NAS-Identifier
- NAS-Ip-Address
- NAS-Port
- NAS-Port-Type
- Message-Authenticator
- Service-Type
- State
- User-Name
- User-Password
- Vendor-specific (Microsoft)
  - MSCHAP-Challenge
  - MSCHAP-Response
  - MSCHAPv2-Response
- Vendor-specific (WISPr)
  - Location-Name
  - Location-ID
  - Logoff-url

Access Accept

- Class
- EAP-Message
- Session-Timeout
- Vendor-specific (Colubris)
  - Colubris AV-Pair

Access Reject

No attributes are supported.

Access Challenge

No attributes are supported.

Accounting Request

- Acct-Authentic
- Acct-Delay-Time
- Acct-Event-Timestamp
- Acct-Session-Id
- Acct-Status-Type
- Called-Station-Id
- Calling-Station-Id
- Class
- Framed-IP-Address
- NAS-Identifier
- NAS-Ip-Address
- NAS-Port
- NAS-Port-Type
- User-Name

Accounting Response

No attributes are supported.

Access request

Acct-Session-Id
(32-bit unsigned integer)
Random value generated per authentication by the service controller.

Called-Station-Id
(string)
By default, this is set to the MAC address of the service controller wireless/LAN port in IEEE format. For example: 00-02-03-5E-32-1A. To use the MAC address of the Internet port, you must edit the config file and change the setting of **radius-called-station-id-port** to **WAN** in the <ACCESS-CONTROLLER> section.

Calling-Station-Id
(string)
The MAC address of the service controller LAN port in IEEE format. For example: 00-02-03-5E-32-1A.

CHAP-Challenge
(string)
Randomly generated by the product. As defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to CHAP. Length = 19 bytes.

CHAP-Password
(string)
The password assigned to the service controller on the **Public access > Attributes** page. Encoded as defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to CHAP.

Connect-Info
(string)
The string “HTTPS”.

EAP-Message
(string)
As defined in RFC 2869. Only present when the authentication method for the RADIUS profile is set to EAP-MD5.

Framed-IP-Address
(32-bit unsigned integer)
IP Address of the service controller LAN port.

Framed-MTU
(32-bit unsigned integer)
Hard-coded to 1496 (802.1X). Hard-coded value of 1496. The value is always four bytes lower than the wireless MTU maximum which is 1500 bytes in order to support IEEE802dot1x authentication.

NAS-Identifier
(string)
The NAS ID set on the **Service Controller >> Authentication > RADIUS profiles > Add New Profile** page for the RADIUS profile being used.

NAS-Ip-Address
(32-bit unsigned integer)
The IP address of the port the service controller is using to communicate with the RADIUS server.

NAS-Port
(32-bit unsigned integer)
Always 0.

NAS-Port-Type
(32-bit unsigned integer)
Always set to 19, which represents WIRELESS_802_11.

Message-Authenticator
(string)
As defined in RFC 2869. Always present even when not doing an EAP authentication. length = 16 bytes.

Service-Type
(32-bit unsigned integer)
RADIUS service type.

State
(string)
As defined in RFC 2865.

User-Name
(string)
The RADIUS username assigned to the service controller on the **Public access > Attributes** page.

User-Password
(string)
The password assigned to the service controller on the **Public access > Attributes** page. Encoded as defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to PAP.

Vendor-specific (Microsoft)
HP ProCurve supports the following Microsoft vendor-specific attributes.

> **MSCHAP-Challenge**
> *(string)*
> As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1 or MSCHAPv2. Length = 8 bytes.

MSCHAP-Response
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1. Length = 49 bytes.

MSCHAPv2-Response
(string)
As defined in RFC 2759. Only present when the authentication method for the RADIUS profile is set to MSCHAPv2. Length = 49 bytes.

Vendor-specific (WISPr)
HP ProCurve supports the following Wi-Fi Alliance vendor-specific attributes.

Location-Name
The WISPr location name assigned to the service controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 2
- Attribute type: A string in the format: `wispr-location-name=`*`location_name`*

Location-ID
The WISPr location name assigned to the service controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 1
- Attribute type: A string in the format: `wispr-location-id=`*`location_id`*

Logoff-url
The WISPr log-off URL that will be used.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 3
- Attribute type: A string in the format: `wispr-logoff-url=`*`URL`*

Access accept

Class
(string)
As defined in RFC 2865. Multiple instances are supported.

EAP-Message
(string)
Only supported when authentication is EAP-MD5. Note that the content will not be read as the RADIUS Access Accept overrides whatever indication is contained inside this packet.

Session-Timeout
(32-bit unsigned integer)
The service controller will retrieve RADIUS attributes when this timer expires. Omitting this attribute or specifying **0** disables the feature. (Note that this is configurable directly on the service controller by setting **Public access > Attributes** > **Retrieval interval**.

Vendor-specific (Colubris)

Colubris AV-Pair
(string)
HP ProCurve has defined this vendor-specific attribute to support configuration of special features on the service controller, such as the customization of the public access interface and global user session settings. This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type: A string in the following format `<keyword>=<value>`

Multiple instances of the Colubris AV-pair can be defined in a RADIUS account to configure a variety of settings. For a complete list of all supported attributes, see *Colubris AV-Pair attribute - Site values on page 9-29*.

Access reject

No attributes are supported.

Access challenge

No attributes are supported.

Accounting request

Acct-Authentic
(32-bit unsigned integer)
Always set to 1 which means RADIUS.

Acct-Delay-Time
(32-bit unsigned integer)
As defined in RFC 2869.

Acct-Event-Timestamp
(32-bit unsigned integer)
As defined in RFC 2869.

Acct-Session-Id
(32-bit unsigned integer)
Random value generated by the service controller.

Acct-Status-Type
(32-bit unsigned integer)
Supported values are: Accounting-On (7) and Accounting-Off (8).

Called-Station-Id
(string)
The MAC address of the service controller LAN port in IEEE format. For example: 00-02-03-5E-32-1A.

Calling-Station-Id
(string)
The MAC address of the service controller LAN port in IEEE format. For example: 00-02-03-5E-32-1A.

Class
(string)
As defined in RFC 2865. Multiple instances are supported.

Framed-IP-Address
(32-bit unsigned integer)
IP Address of the service controller LAN port.

NAS-Identifier
(string)

The NAS ID for the RADIUS profile being used.

NAS-Ip-Address
(32-bit unsigned integer)
The IP address of the port the service controller is using to communicate with the RADIUS server.

NAS-Port
(32-bit unsigned integer)
Always 0.

NAS-Port-Type
(32-bit unsigned integer)
Always set to 19, which represents WIRELESS_802_11.

User-Name
(string)
The RADIUS username assigned to the service controller on the **Public access > Attributes** page.

Accounting response

No attributes are supported.

User attributes

The following attributes are supported for user accounts.

Access Request

- Acct-Session-Id
- Called-Station-Id
- Calling-Station-Id
- CHAP-Challenge
- CHAP-Password
- Chargeable User Identity (CUI)
- Connect-Info
- EAP-Message
- Framed-IP-Address
- Framed-MTU
- NAS-Identifier
- NAS-Ip-Address
- NAS-Port
- NAS-Port-Type
- Message-Authenticator
- Service-Type
- State
- User-Name
- User-Password
- Vendor-specific (Microsoft)
  - MSCHAP-Challenge
  - MSCHAP-Response
  - MSCHAPv2-Response
- Vendor-specific (WISPr)
  - Location-Name
  - Location-ID
  - Logoff-url

Access Accept

- Acct-Interim-Interval
- Chargeable User Identity (CUI)
- Class
- EAP-Message
- Idle-Timeout
- Reply-Message
- Session-Timeout
- Termination-Action
- Tunnel-Medium-Type
- Tunnel-Private-Group-ID
- Tunnel-Type
- Vendor-specific (Microsoft)
  - MS-MPPE-Recv-Key
  - MS-MPPE-Send-Key
- Vendor-specific (Colubris)
  - Colubris AV-Pair
  - Colubris-Intercept

Access Reject

- EAP-Message
- Vendor-specific (Microsoft)
  - MSCHAP-Error
- Reply-Message

Access Challenge

- EAP-Message
- State

Accounting Response

No attributes are supported.

Accounting Request

- Acct-Authentic
- Acct-Delay-Time
- Acct-Event-Timestamp
- Acct-Session-Id
- Acct-Status-Type
- Calling-Station-Id
- Called-Station-Id
- Chargeable User Identity (CUI)
- Class
- Framed-IP-Address
- NAS-Identifier
- NAS-Ip-Address
- NAS-Port
- NAS-Port-Type
- User-Name
- Vendor-specific (WISPr)
  - Location-Name
  - Location-ID
  - Logoff-url
- Acct-Session-Time
- Acct-Input-Gigawords
- Acct-Input-Octets
- Acct-Input-Packets
- Acct-Output-Gigawords
- Acct-Output-Octets
- Acct-Output-Packets
- Acct-Terminate-Cause

Access request

Acct-Session-Id
(32-bit unsigned integer)
Random value generated per authentication by the service controller.

Called-Station-Id
(string)
By default, this is set to the MAC address of the service controller wireless/LAN port in IEEE format. For example: 00-02-03-5E-32-1A. To use the MAC address of the Internet port, you must edit the config file and change the setting of **radius-called-station-id-port** to **WAN** in the <ACCESS-CONTROLLER> section. If location-aware authentication is enabled for the VSC the user is logged into, then this value is defined by the VSC.

Calling-Station-Id
(string)
The MAC address of the user's station in IEEE format. For example: 00-02-03-5E-32-1A.

CHAP-Challenge
(string)
Randomly generated. As defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to CHAP. Length = 19 bytes.

CHAP-Password
(string)
The user's password. Encoded as defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to CHAP.

Chargeable User Identity (CUI)
(string)
As defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

Connect-Info
(string)
The string "HTTPS" or "IEEE802.1X".

EAP-Message
(string)
As defined in RFC 2869. Only present when the authentication method for the RADIUS profile is set to EAP-MD5.

Framed-IP-Address
(32-bit unsigned integer)
IP Address as configured on the client station (if known by the service controller).

Framed-MTU
(32-bit unsigned integer)
Hard-coded value of 1496. The value is always four bytes lower than the wireless MTU maximum which is 1500 bytes in order to support IEEE802dot1x authentication.

NAS-Identifier
(string)
The NAS ID set on the **Service Controller >> Authentication > RADIUS profiles > Add New Profile** page for the RADIUS profile being used.

NAS-Ip-Address
(32-bit unsigned integer)
The IP address of the port the service controller is using to communicate with the RADIUS server.

NAS-Port
(32-bit unsigned integer)
A port number, other than 0.

NAS-Port-Type
(32-bit unsigned integer)
Always set to 19, which represents WIRELESS_802_11.

Message-Authenticator
(string)
As defined in RFC 2869. Always present even when not doing an EAP authentication. length = 16 bytes.

Service-Type
(32-bit unsigned integer)
RADIUS service type.

State
(string)
As defined in RFC 2865.

User-Name
(string)
The username assigned to the user or a device when using MAC authentication.

User-Password
(string)
The password supplied by a user or device when logging in. Encoded as defined in RFC 2865. Only present when the authentication method for the RADIUS profile is set to PAP.

Vendor-specific (Microsoft)
HP ProCurve supports the following Microsoft vendor-specific attributes.

MSCHAP-Challenge
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1 or MSCHAPv2. Length = 8 bytes.

MSCHAP-Response
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1. Length = 49 bytes.

MSCHAPv2-Response
(string)
As defined in RFC 2759. Only present when the authentication method for the RADIUS profile is set to MSCHAPv2. Length = 49 bytes.

Vendor-specific (WISPr)
HP ProCurve supports the following Wi-Fi Alliance vendor-specific attributes.

Location-Name
The WISPr location name assigned to the service controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 2
- Attribute type: A string in the format: `wispr-location-name=`*`location_name`*

Location-ID
The WISPr location name assigned to the service controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 1
- Attribute type: A string in the format: `wispr-location-id=`*`location_id`*

Logoff-url
The WISPr log-off URL that will be used.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 3
- Attribute type: A string in the format: `wispr-logoff-url=`*`URL`*

Access accept

Acct-Interim-Interval
(32-bit unsigned integer)
When present, enables the transmission of RADIUS accounting requests of the Interim Update type. Specify the number of seconds between each transmission.

Chargeable User Identity (CUI)
(string)
As defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

Class
(string)
As defined in RFC 2865. Multiple instances are supported.

EAP-Message
(string)
Only supported when authentication is EAP-MD5. Note that the content will not be read as the RADIUS Access Accept overrides whatever indication is contained inside this packet.

Idle-Timeout
(32-bit unsigned integer)
Maximum idle time in seconds allowed for the user. Once reached, the user session is terminated with termination-cause IDLE-TIMEOUT. Omitting the attribute or specifying 0 disables the feature.

Reply-Message
(string)
This string (as defined in RFC 2865) is recorded and passed as is to the GetRadiusReplyMessage() asp function. Multiple string are supported to a maximum length of 252 bytes.

Session-Timeout
(32-bit unsigned integer)
Maximum time a session can be active. The user must re-authenticate when this timer expires. Omitting this attribute or specifying **0** disables the feature.

Termination-Action
(32-bit unsigned integer)
As defined by RFC 2865. If set to **1**, a new Access Request is sent. If an Access Accept is returned, the service controller then extends the user's session timeout, and if applicable, session quota, according the value returned by the RADIUS server.

Tunnel-Medium-Type
(24-bit unsigned integer)
Only used when assigning a specific VLAN number to a user. In this case it must be set to 802.

Tunnel-Private-Group-ID
(string)
Only used when assigning a specific VLAN number to a user. In this case it must be set to the VLAN ID.

Tunnel-Type
(24-bit unsigned integer)
Only used when assigning a specific VLAN number to a user. In this case it must be set to 13 (VLAN).

Vendor-specific (Microsoft)
HP ProCurve supports the following Microsoft vendor-specific attributes.

MS-MPPE-Recv-Key
(string)
Use to validate a PMKID inside a 802.11 association request, send EAPOL keys to a wireless station when a VSC has 802.1X WEP enabled, and to perform a four-way handshake.

MS-MPPE-Send-Key
(string)
Use to validate a PMKID inside a 802.11 association request, send EAPOL keys to a wireless station when a VSC has 802.1X WEP enabled, and to perform a four-way handshake.

Vendor-specific (Colubris)
(string)

Colubris AV-Pair
HP ProCurve has defined a vendor-specific attribute to support configuration of user session settings. This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type: A string in the following format `<keyword>=<value>`

Multiple instances of the Colubris AV-Pair can be defined in a RADIUS account to configure a variety of settings. For a complete list of all supported settings, see *Colubris AV-Pair attribute - Site values on page 9-29*.

Colubris-Intercept
This attribute is used to enable/disable the interception and redirection of traffic for individual users. The destination for intercepted traffic is defined separately for each VSC using the **Interception** option under **VSC egress mapping.** See *VSC egress mapping on page 2-11*.

You may need to define the Colubris-Intercept attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 1
- Attribute type = integer with one of the following values:
  - **0**: Do not intercept user traffic.
  - **1**: Intercept user traffic and redirect it to the destination defined by the **Intercepted** option under **VSC egress mapping** in the VSC to which the user is connected.

Access reject

EAP-Message
(string)
Only supported when authentication is EAP-MD5. Note that the content will not be read as the RADIUS Access Reject overrides whatever indication is contained inside this packet.

Vendor-specific (Microsoft)
HP ProCurve supports the following Microsoft vendor-specific attributes.

MSCHAP-Error
(string)
A MSCHAP specific error as defined by RFC 2433.

Reply-Message
(string)
This string (as defined in RFC 2865) is recorded and passed as is to the GetRadiusReplyMessage() asp function. Multiple string are supported to a maximum length of 252 bytes.

Access challenge

EAP-Message
(string)
One or more occurrences of this attribute is supported inside the same packet. All occurrences are concatenated and transmitted to the IEEE802dot1x client as is. As defined in RFC 2869.

State
(string)
As defined in RFC 2865.

Accounting request

Accounting start, stop. and interim-update

Acct-Authentic
(32-bit unsigned integer)
Always set to 1 which means RADIUS.

Acct-Delay-Time
(32-bit unsigned integer)
As defined in RFC 2869.

Acct-Event-Timestamp
(32-bit unsigned integer)
As defined in RFC 2869.

Acct-Session-Id
(32-bit unsigned integer)
Random value generated by the service controller.

Acct-Status-Type
(32-bit unsigned integer)
Supported value are: Start (1), Interim Update (3), and Stop (2).

Calling-Station-Id
(string)
The MAC address of the user's computer in IEEE format. For example: 00-02-03-5E-32-1A.

Called-Station-Id
(string)
The MAC address of the service controller LAN port in IEEE format. For example: 00-02-03-5E-32-1A.

Chargeable User Identity (CUI)
(string)
As defined in RFC-4372. The CUI is used to associate a unique identifier with a user so that the user can be identified (for billing, authentication or other purposes) when roaming outside of their home network.

Class
(string)
As defined in RFC 2865. Multiple instances are supported.

Framed-IP-Address
(32-bit unsigned integer)
IP Address of the user's computer.

NAS-Identifier
(string)

The NAS ID for the RADIUS profile being used.

NAS-Ip-Address
(32-bit unsigned integer)
The IP address of the port the service controller is using to communicate with the RADIUS server.

NAS-Port
(32-bit unsigned integer)
A virtual port number starting at 1. Assigned by the service controller.

NAS-Port-Type
(32-bit unsigned integer)
Always set to 19, which represents WIRELESS_802_11.

User-Name
(string)
The username assigned to the user or to a device when using MAC authentication.

Vendor-specific (WISPr)
HP ProCurve supports the following Wi-Fi Alliance vendor-specific attributes.

Location-Name
The WISPr location name assigned to the service controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 2
- Attribute type: A string in the format: `wispr-location-name=`*`location_name`*

Location-ID
The WISPr location name assigned to the service controller.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 1
- Attribute type: A string in the format: `wispr-location-id=`*`location_id`*

Logoff-url
The WISPr log-off URL that will be used.

- SMI network management private enterprise code = 14122
- Vendor-specific attribute type number = 3
- Attribute type: A string in the format: `wispr-logoff-url=`*`URL`*

Accounting stop. and interim-update

Acct-Session-Time
(32-bit unsigned integer)
Number of seconds this session since this session was authenticated. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Input-Gigawords
(32-bit unsigned integer)
High 32-bit value of the number of octets/bytes received by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Input-Octets
(32-bit unsigned integer)
Low 32-bit value of the number of octets/bytes received by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Input-Packets
(32-bit unsigned integer)
Low 32-bit value of the number of packets/bytes received by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Output-Gigawords
(32-bit unsigned integer)
High 32-bit value of the number of octets/bytes sent by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**. As defined in 2869.

Acct-Output-Octets
(32-bit unsigned integer)
Low 32-bit value of the number of octets/bytes sent by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Acct-Output-Packets
(32-bit unsigned integer)
Low 32-bit value of the number of packets/bytes sent by the user. Only present when **Acct-Status-Type** is **Interim-Update** or **Stop**.

Accounting stop only

Acct-Terminate-Cause
(32-bit unsigned integer)
Termination cause for the session See RFC 2866 for possible values. Only present when **Acct-Status-Type** is **Stop**.

ID	Cause	Notes
1	User Request	Supported. Indicates that the user logged out.
2	Lost Carrier	Supported. Indicates that the client station is no longer alive.
3	Lost Service	Supported. When location-aware is enabled and a user switches access points, the service controller re-authenticates the user. If authentication fails due to timeout, this code is returned.
4	Idle Timeout	Supported. User exceeded the idle timeout value defined for the session.
5	Session Timeout	Supported. User exceeded maximum time defined for the session.
6	Admin Reset	Supported. User session was terminated by the service controller administrator via SNMP or the management tool.
7	Admin Reboot	Not Supported. (not applicable)
8	Port Error	Supported. If two users are detected using the same IP address, both are logged out with this error. Another cause is if an error is encountered in an access list definition. For example, an invalid host was specified.
9	NAS Error	Not Supported. (not applicable)
10	NAS Request	Not Supported. (not applicable)
11	NAS Reboot	Supported. User was logged out because the service controller was restarted.
12	Port Unneeded	Not Supported. (not applicable)
13	Port Preempted	Supported. When a user switches AP or SSID with incompatible configurations (authentication type), they are logged out with this code. Also if the user changes authentication type of the same AP.
14	Port Suspended	Not Supported. (not applicable)
15	Service Unavailable	Not Supported. (not applicable)
16	Callback	Not Supported. (not applicable)

ID	Cause	Notes
17	User Error	Supported. An 802.1X client initiated a second authentication request for a user, and this request was refused.
18	Host Request	Not Supported. (not applicable)
0x8744 (34628 decimal)	Termination	HP ProCurve Networking-specific termination cause.

Accounting response

No attributes are supported.

Administrator attributes

If you want to support multiple administrator names and passwords, you must use a RADIUS server to manage them. The service controller only supports a single admin name and password internally (defined on the **Management > Management tool** page).

Note

Improper configuration of the administrator profile could expose the service controller to access by any user with a valid account. The only thing that distinguishes an administrative account from that of a standard user account is the setting of the service type. Make sure that a user is not granted access if service type is not Administrative, This is the reason why it may be prudent to use a different RADIUS server to handle administrator logins. This practice reduces the risk of a bad configuration on the RADIUS server side creating a security hole.

The following attributes are supported for administrator accounts.

Access Request

- Framed-MTU
- NAS-Identifier
- User-Name
- Service-Type
- Vendor-specific (Microsoft)
  - MSCHAP-Challenge
  - MSCHAP-Response

Access Accept

- Vendor-specific (Colubris)

Access Reject

No attributes are supported.

Access Challenge

No attributes are supported.

Accounting Request

No attributes are supported.

Accounting Response

No attributes are supported.

Access request

Framed-MTU
(32-bit unsigned integer)
Hard-coded value of 1496. The value is always four bytes lower than the wireless MTU maximum which is 1500 bytes in order to support IEEE802dot1x authentication.

NAS-Identifier
(string)
The NAS ID set on the **Service Controller >> Authentication > RADIUS profiles > Add New Profile** page for the RADIUS profile being used.

User-Name
(string)
The username assigned to the administrator.

Service-Type
(32-bit unsigned integer)
As defined in RFC 2865. Set to a value of 6, which indicates SERVICE_TYPE_ADMINISTRATIVE.

Vendor-specific (Microsoft)
HP ProCurve supports the following Microsoft vendor-specific attributes.

MSCHAP-Challenge
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1 or MSCHAPv2. Length = 8 bytes.

MSCHAP-Response
(string)
As defined in RFC 2433. Only present when the authentication method for the RADIUS profile is set to MSCHAPv1. Length = 49 bytes.

Access accept

Vendor-specific (Colubris)
(string)

Colubris AV-Pair
HP ProCurve has defined a vendor-specific attribute to support configuration of user session settings. This attribute conforms to RADIUS RFC 2865. You may need to define this attribute on your RADIUS server (if it is not already present) using the following values:

- SMI network management private enterprise code = 8744
- Vendor-specific attribute type number = 0
- Attribute type: A string in the following format `<keyword>=<value>`

Multiple instances of the Colubris AV-Pair can be defined in a RADIUS account to configure a variety of settings. For a complete list of all supported attributes, see *Colubris AV-Pair attribute - Administrator values on page 9-69*.

Colubris AV-Pair attribute - Site values

Site values let you define global settings that affect operation of the public access network and all user accounts.

Each Colubris AV-Pair value is specified using the following format: `<keyword>=<value>`

The following table lists all supported site value keywords and provides a link to complete descriptions for each one.

Colubris AV-Pair keyword	For more information see
access-list use-access-list=uselistname use-access-list-unauth=uselistname default-user-access-list	*Access list on page 9-30*
configuration-file	*Configuration file on page 9-41*
ssl-certificate	*Custom SSL certificate on page 9-41*
custom-pages	*Loading custom pages from an archive on page 9-42*
login-page transport-page session-page fail-page logo	*Loading individual pages on page 9-43*
welcome-url login-err goodbye-url	*Hosting pages on an external Web server on page 9-44*
login-url	*Remote login page on page 9-44*
messages	*Custom message file on page 9-48*
default-user-acct-interim-update	*Default user interim accounting update interval on page 9-48*
default-user-bandwidth-level	*Default user bandwidth level on page 9-49*
default-user-idle-timeout	*Default user idle timeout on page 9-49*
default-user-one-to-one-nat	*Default user one-to-one NAT on page 9-50*
default-user-use-public-ip-subnet	*Default user public IP address on page 9-51*

Colubris AV-Pair keyword	For more information see
default-user-session-timeout	*Default user session timeout on page 9-51*
default-user-smtp-redirect	*Default user SMTP server on page 9-51*
default-user-welcome-url default-user-goodbye-url	*Default user URLs on page 9-52*
default-user-max-input-packets default-user-max-output-packets default-user-max-total-packets default-user-max-input-octets default-user-max-output-octets default-user-max-total-octets	*Default user quotas on page 9-49*
default-user-max-input-rate=value default-user-max-output-rate=value	*Default user data rates on page 9-50*
http-proxy-upstream	*HTTP proxy upstream on page 9-52*
ipass-login-url	*IPass login URL on page 9-53*
mac-address	*MAC authentication on page 9-53*
primary-web-server-status-url secondary-web-server-status-url primary-web-server-status-url secondary-web-server-status-url	*Multiple login servers on page 9-54*
redirect-url	*Redirect URL on page 9-56.*
ssl-noc-certificate ssl-noc-ca-certificate	*NOC authentication on page 9-59.*
wispr-login-url wispr-abort-login-url redirect-page access-procedure	*ProCurve WISPr support on page 9-59.*
dnat-server primary-dnat-server-status-url secondary-dnat-server-status-url	*Traffic forwarding (dnat-server) on page 9-60.*

Access list

Access lists enable you to create public areas on your network that all users can browse, and protected areas that are restricted to specific user accounts or groups.

Each access list is a set of rules that governs how the service controller controls access to network resources. You can create multiple access lists, each with multiple rules to manage the traffic on your public access network.

Default setting

By default no access lists are defined. This means that:

- If authentication (802.1X, WPA, HTML, MAC) is not enabled on a VSC, all users that connect to the VSC have access to the protected network.
- If authentication (802.1X, WPA, HTML, MAC) is enabled on a VSC, then:
  - Unauthenticated users only reach the public access login page. Access to the protected network is blocked, except for **register.procurve.com** which enables product registration.
  - Authenticated users have access to the protected network.

Note If you only enable MAC-based authentication on a VSC, wired users are not required to authenticate and gain access to the protected network. In this case it is important to restrict network access with the appropriate access list definition.

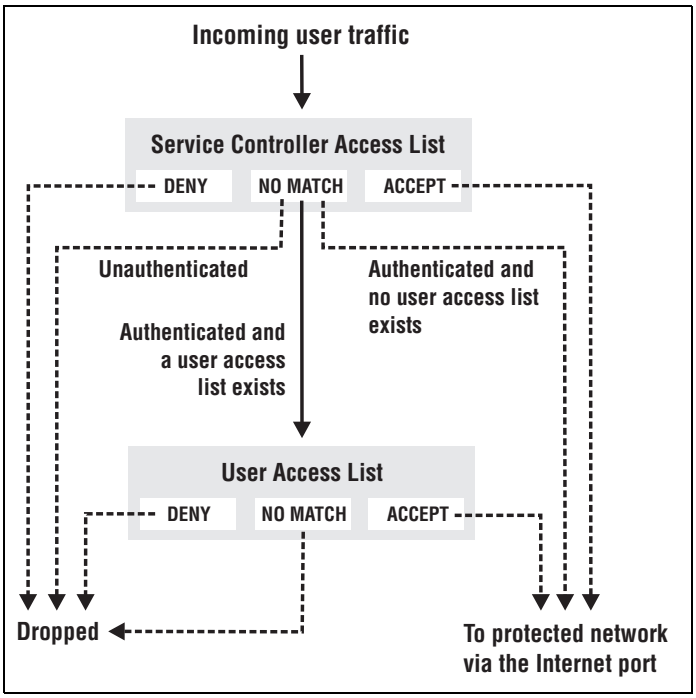
How the access lists work

Access lists can be applied on the service controller (site access lists), in which case they affect all user traffic, or individually for each user account (user access lists).

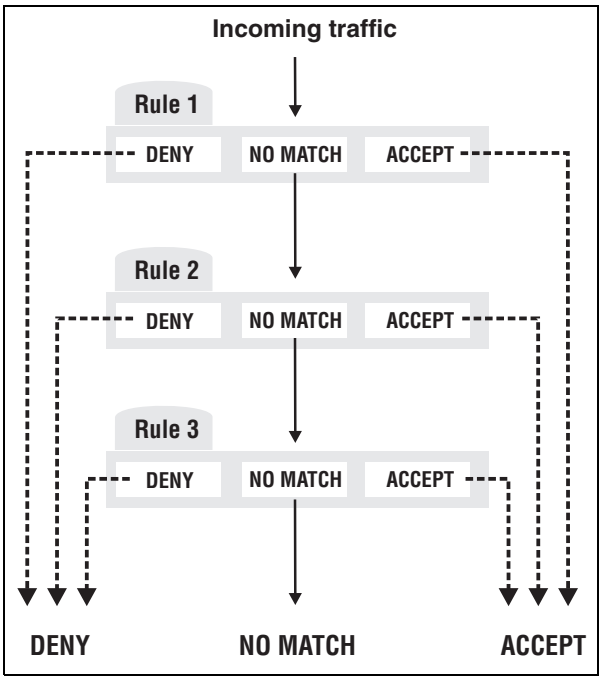
Incoming traffic cascades through the currently active lists. Traffic that is accepted or denied by a list is not available to the list that follows it. Traffic that passes through all lists without being accepted or denied is dropped.

- Access list rules that **accept** traffic are: ACCEPT, ACCEPT-MORE, DNAT-SERVER, and REDIRECT.
- Access list rules that **deny** traffic are: DENY and WARN.

The following diagram illustrates how incoming traffic from a user session is processed by the access list mechanism.



Within each access list, traffic cascades through the list rules in a similar manner.



Access list rules are numbered according to the order in which they are specified. Only data that is not accepted or denied by a rule is available to the next rule in the list.

Accounting support

Each rule in an access list can be configured with an account name for billing purposes. The service controller sends billing information based on the amount of traffic matched by the rule.

This lets you create rules to track and bill traffic to particular destinations.

Tips on using the access list

With certificates

- If you replaced the default SSL certificate on the service controller with one signed by a well-known CA, you should define the access list to permit access to the CA certificate for all non-authenticated users. This enables the user's browser to verify that the certificate is valid without displaying any warning messages.
- Users may have configured their Web browsers to check all SSL certificates against the Certificate Revocation List (CRL) maintained by the CA that issued the certificate. The location of the CRL may be configured in the browser, or embedded in the certificate. The access list should be configured to permit access to the CRL, otherwise the user's browser times out before displaying the login page.

Remote login page

If you are using the remote login page feature, make sure that access to the Web server hosting the login page is granted to all unauthenticated users via the site access list.

SMTP redirect

If an unauthenticated user establishes a connection to their email server, the SMTP redirect feature will not work once the user logs in. The user's email is still sent to the original email server.

To avoid this, do not use an access list to open TCP port 25 for unauthenticated users.

Critical access list definitions (such as for a remote login page, certificates) should not use the OPTIONAL setting because if these definitions fail to initialize there is no indication in the log.

Defining access lists

Access lists are defined by adding the following Colubris AV-Pair value string to the RADIUS profile for a service controller or to the local list (**Public access > Attributes** page).

```
access-list=value
```

Each value string defines one rule. Up to 99 rules can be defined for an access list.

All rules that make up an access list must be initialized without error for the list to be active. (You can force the service controller to ignore initialization errors on a rule-by-rule basis by using the OPTIONAL parameter.)

You can define up to 32 access lists.

Activating site access lists

When an access list is activated on the service controller, it applies to all access controlled user traffic handled by the service controller.

Access lists are activated by adding the following Colubris AV-Pair value string to the RADIUS profile for a service controller or to the local list (**Public access > Attributes** page).

```
use-access-list=uselistname
```

Only one access list can be active on the service controller. This list must be initialized without an error.

It is possible to set an access list to apply only for unauthenticated users by specifying the following value string:

```
use-access-list-unauth=uselistname
```

User access lists

Access lists can also be activated on a per-user basis by configuring the appropriate settings for each user account. See *Access list on page 9-64* for more information.

A default access list can defined by adding the following Colubris AV-Pair value string to the RADIUS profile for a service controller or to the local list (**Public access > Attributes** page). This defines the access list to use for all users whose profiles do not contain an access list value.

```
default-user-access-list=uselistname
```

Syntax

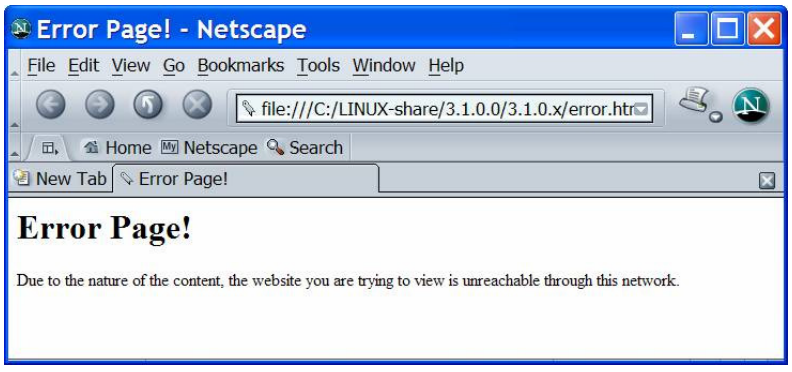
```
access-list=
listname[,OPTIONAL],action,protocol,address,port[,account[,interval]]

use-access-list=uselistname

default-user-access-list=uselistname

use-access-list-unauth=uselistname
```

Note You can use spaces as separators instead of commas.

Where:

Parameter	Description
`listname`	Specify a name (up to 32 characters long) to identify the access list this rule applies to. If a list with this name does not exist, a new list is created. If a list with this name exists, the rule is added to it.
`uselistname`	Specify the name of an existing access list. This list is activated for the current profile. Lists are checked in the order they are activated.
`OPTIONAL`	Allows the access list to be activated even if this rule fails to initialize. For example, if you specify a rule that contains an *address* which cannot be resolved for some reason, the other rules that make up the access list will still be initialized. If you do not specify optional, a failed rule will cause the entire list to fail. **Critical access list definitions (such as for a remote login page, certificates) should not use the OPTIONAL setting because if these definitions fail to initialize there will be no indication in the log.**

Parameter	Description

`action`	Specify what action the rule takes when it matches incoming traffic. The options are:
	■ `ACCEPT` - Allow traffic matching this rule.
	■ `ACCEPT-MORE` - Allow traffic matching this rule and allocate extra connections (when required) to enable users to connect with the specified *address*.
	By default the service controller allows up to 200 TCP or UDP connections per authenticated or unauthenticated user. If a user has exceeded this connection limit, this parameter allows the service controller to permit extra connections from the user when connecting to the specified destination. Connections are assigned from a global pool of 100 connections.
	This can be used to make sure that users can always reach an important resource on the network. For example, the following access list definition allows additional connections as needed to any user who is trying to reach **my-web-server.com.**
	`access-list=procurve,ACCEPT-MORE,all,my-web-server.com,80`
	`use-access-list=procurve`
	■ `DENY` - Reject traffic matching this rule.
	■ `DNAT-SERVER`: Traffic matching this rule is forwarded to the destination defined by the **dnat-server** value. See *Traffic forwarding (dnat-server) on page 9-60* for more information.
	■ `REDIRECT`: Reject traffic matching this rule and redirect the user's Web browser to the page specified by **redirect-url**, or **login-url** if **redirect-url** is not defined. See *Redirect URL on page 9-56* for more information. For example, one use for this feature could be to block access to a popular protocol, then prompt the user for additional fees to activate support.
	■ `WARN`: Reject traffic matching this rule and return an HTTP error message (which is not customizable) indicating that access to the site is not allowed by the network. For example:
	 

Parameter	Description
`protocol`	Specify the protocol to check: `tcp, udp, icmp, all`
`address`	Specify one of the following: ■ IP address or domain name (up to 107 characters in length) ■ Subnet address. Include the network mask as follows: `address/subnet mask` For example: 192.168.30.0/24 ■ Use the keyword `all` to match any address. ■ Use the wildcard symbol * to match any sequence of characters at the beginning or the end of a domain name. For example: ***.mydomain** matches any host on the domain **.mydomain**. **myhost.*** matches **myhost** at any domain. For example, **myhost.com** or **myhost.ca** ■ Use the keyword `none` if the protocol does not take an address range (ICMP for example).
`port`	Specify a specific port to check or a port range as follows: ■ `none` - Used with ICMP (since it has no ports). ■ `all` - Check all ports. ■ `1-65535[:1-65535]` - Specify a specific port or port range. **Note:** If you choose all possible protocols for an access-list definition, then you must supply all ports as well.
`account`	Specify the name of the user account the service controller will send billing information to for this rule. Account names must be unique and can be up to 32 characters in length.
`interval`	Specify time between interim accounting updates. If you do not enable this option, accounting information is only sent when a user connection is terminated. Range: 5 to 99999 seconds in 15 second increments.

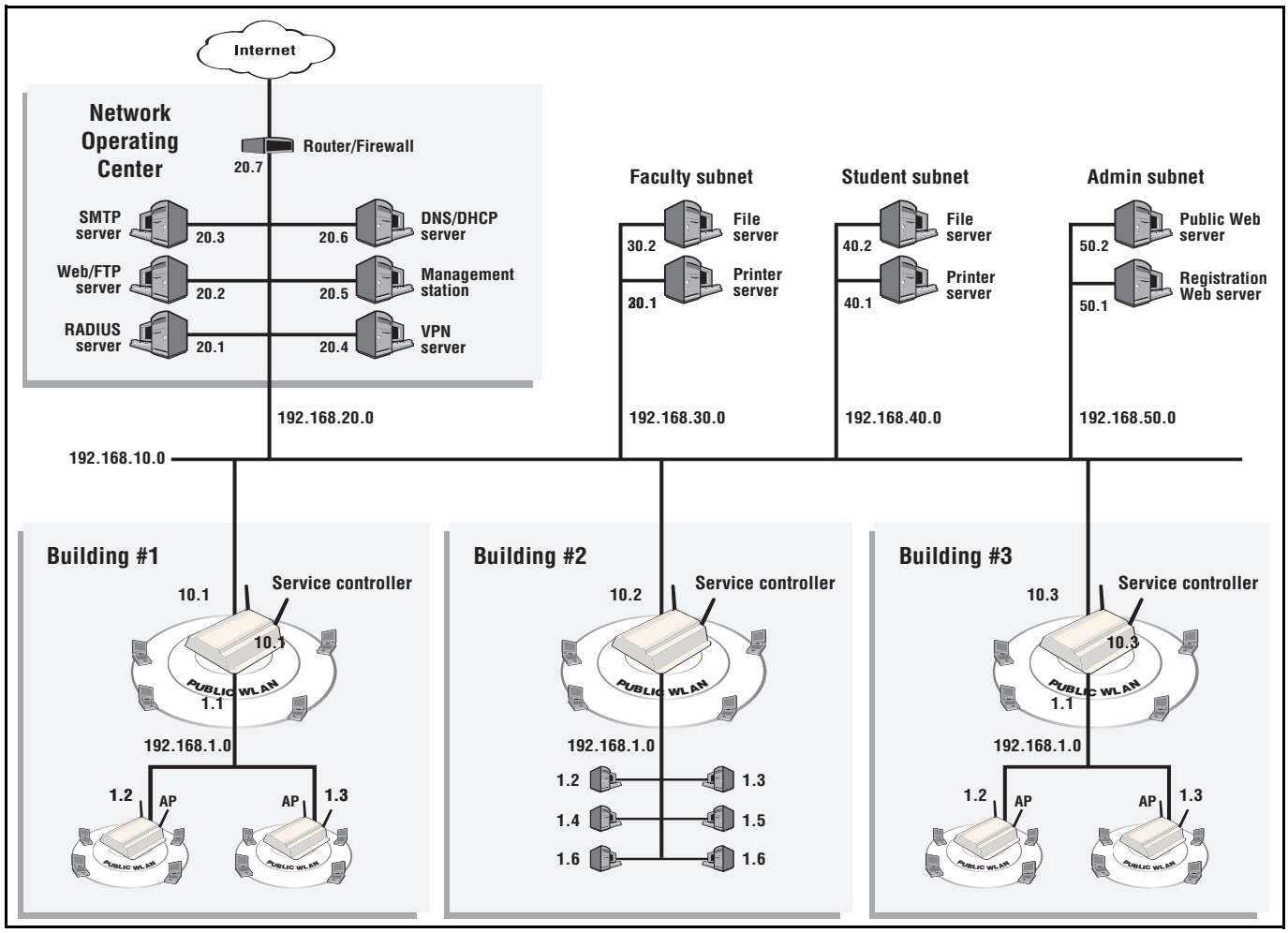
Access list example

This example illustrates how access lists can be used to control access to network resources for different groups of users at a fictitious university campus.

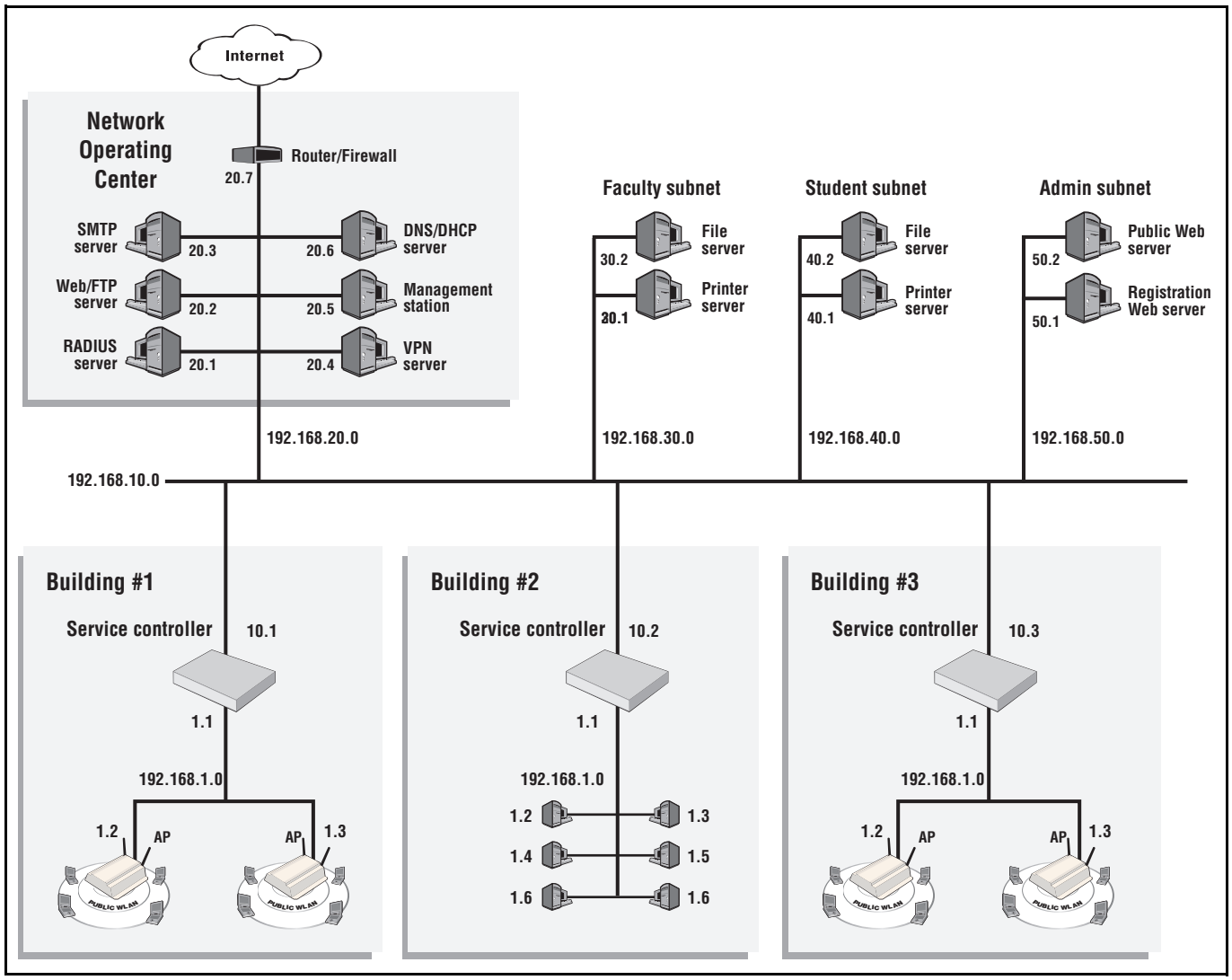
Topology

The following two topologies show potential wireless deployments for the campus using different types of HP ProCurve Networking equipment. In both cases, a RADIUS server is used to store configuration attributes for the public access network. Although the topologies are slightly different, the same access list definitions are used for both installations.

Topology 1:


Internet
Network Operating Center
Router/Firewall
20.7
SMTP server
20.3
DNS/DHCP server
20.6
Web/FTP server
20.2
Management station
20.5
RADIUS server
20.1
VPN server
20.4
192.168.20.0
Faculty subnet
File server
30.2
Printer server
20.1
192.168.30.0
Student subnet
File server
40.2
Printer server
40.1
192.168.40.0
Admin subnet
Public Web server
50.2
Registration Web server
50.1
192.168.50.0
192.168.10.0
Building #1
Service controller
10.1
10.1
PUBLIC WLAN
1.1
192.168.1.0
1.2
AP
AP
1.3
Building #2
Service controller
10.2
PUBLIC WLAN
192.168.1.0
1.2
1.3
1.4
1.5
1.6
1.6
Building #3
Service controller
10.3
10.3
PUBLIC WLAN
1.1
192.168.1.0
1.2
AP
AP
1.3

Topology 2:



Access list definitions

The RADIUS profile for the service controller contains the following:

```
access-list=everyone,ACCEPT,tcp,192.168.50.2,80

access-list=students,ACCEPT,tcp,192.168.50.1,80,students_reg,500
access-list=students,ACCEPT,all,192.168.40.0/24,all
access-list=students,DENY,all,192.168.20.0/24,all
access-list=students,DENY,all,192.168.30.0/24,all
access-list=students,ACCEPT,all,all.all,student_internet_use,5000

access-list=faculty,ACCEPT,tcp,192.168.50.1,80,faculty_reg,500
access-list=faculty,ACCEPT,all,192.168.30.0/24,all
access-list=faculty,DENY,all,192.168.20.0/24,all
access-list=faculty,DENY,all,192.168.40.0/24,all
access-list=faculty,ACCEPT,all,all.all,faculty_internet_use,5000

use-access-list=everyone
```

The RADIUS profile for every student contains the following:

```
use-access-list=students
```

The RADIUS profile for every faculty member contains the following:

```
use-access-list=faculty
```

This definitions create three access lists: everyone, students, and faculty.

Everyone
This list applies to all users (students, teachers, guests), whether they are authenticated or not. This is because the list is active on the service controller, which is accomplished with the entry:

```
use-access-list=everyone
```
It enables everyone to access the public Web server.

Students
This list applies to authenticated students only. It is composed of the following entries:

```
access-list=students,ACCEPT,tcp,192.168.50.1,80,students_reg,500
```
Enables Web traffic to the registration Web server. Accounting data is recorded in the account students_reg.

```
access-list=students,ACCEPT,all,192.168.40.0/24,all
```
Enables traffic to reach the student segment.

```
access-list=students,DENY,all,192.168.20.0/24,all
access-list=students,DENY,all,192.168.30.0/24,all
```
These two entries deny access to the faculty subnet and the NOC.

```
access-list=students,ACCEPT,all,all.all,student_internet_use,5000
```
Enables all other traffic to reach the Internet (via routers on the backbone LAN and the router in the NOC). If this last rule did not exist, this traffic would be dropped.

Faculty
This list applies to authenticated faculty members only. It is composed of the following entries:

```
access-list=faculty,ACCEPT,tcp,192.168.50.1,80,faculty_reg,500
```
Enables Web traffic to the registration Web server. Accounting data is recorded in the account faculty_reg.

```
access-list=faculty,ACCEPT,all,192.168.30.0/24,all
```
Enables traffic to reach the faculty segment.

```
access-list=faculty,DENY,all,192.168.20.0/24,all
access-list=faculty,DENY,all,192.168.40.0/24,all
```
These two entries deny access to the student subnet and the NOC.

```
access-list=faculty,ACCEPT,all,all.all,faculty_internet_use,5000
```
Enables all other traffic to reach the Internet (via routers on the backbone LAN and the router in the NOC). If this last rule did not exist, this traffic would be dropped.

Configuration file

The service controller can retrieve and load a new configuration file automatically, based on the URL you specify.

Syntax

```
configuration-file=URL[placeholder]
```

Where:

Parameter	Description
`URL`	Specify the URL that points to the new configuration file.

By using the following placeholder, you can customize the URL for each service controller. This is useful when you need to update multiple units.

Placeholder	Description
`%n`	Returns the NAS ID assigned to the service controller. By default, this is the unit serial number.
`%s`	Returns the RADIUS login name assigned to the service controller on the **Public access > Attributes** page. By default, this is the unit serial number.
`%i`	Returns the domain name assigned to the service controller Internet port.
`%a`	Returns the IP address of the service controller Internet port.

Custom SSL certificate

The service controller can retrieve a custom SSL security certificate to replace the HP ProCurve certificate that is included by default.

Syntax

```
ssl-certificate=URL[placeholder]
```

Where:

Parameter	Description
`URL`	Specify the URL that points to the new certificate.

By using the following placeholder, you can customize the URL for each service controller. This is useful when you need to update multiple units.

Placeholder	Description
`%n`	Returns the NAS ID assigned to the service controller. By default, this is its serial number.
`%s`	Returns the RADIUS login name assigned to the service controller. By default, this is its serial number.
`%i`	Returns the domain name assigned to the service controller Internet port.
`%a`	Returns the IP address of the service controller Internet port.

The certificate is encoded using PKCS#12 format, and contains:

- the private key of the Web server
- the certificate of the Web server

The file is locked using a password.

Note The password with which the certificate was locked must be the same as the password specified on the **Public access > Attributes** page. This is the password the service controller uses to login to the RADIUS server.

Example

```
ssl-certificate=http://www.mycompany.com/%s_certificate
```

Custom public access interface Web pages

Several options are available to define custom pages.

Loading custom pages from an archive

This option enables you load site files from an external file archive, allowing you to replace the entire public access Web site in one simple operation. The archive must be in .zip format.

Note The contents of the existing public access site is deleted and replaced by the contents of the archive (.zip) file. If the archive does not contain a complete set of valid pages, the public access interface will not function correctly.

Note When unzipped the total size of all files must be less than 1MB.

Syntax

```
custom-pages=ArchiveURL
```

Where:

Parameter	Description
`ArchiveURL`	URL of the .zip archive to be loaded.

Loading individual pages

Use the following values to retrieve pages from an external location and load them onto the service controller. For descriptions of the individual pages see *Current site files on page 8-22*.

Note These pages can only be changed as a group. You cannot, for example, just specify the login-page value. You must specify all of the following.

Note The maximum length of any page URL is 512 characters. If this is exceeded (when using placeholders for example), the URL is truncated. Therefore, it is recommended that you specify the most-important placeholders first.

Login page

`login-page=`*`URL_of_page`* `[placeholder]`

Can be omitted if a remote login page is being used. See *Remote login page on page 9-44*.

Transport page

`transport-page=`*`URL_of_page`* `[placeholder]`

Session page

`session-page=`*`URL_of_page`* `[placeholder]`

Fail page

`fail-page=`*`URL_of_page`* `[placeholder]`

Logo

`logo=`*`URL_of_gif_file`* `[placeholder]`

Placeholders

The following placeholder is only available when using a RADIUS server. If these values are specified under **Public access > Attributes > Configured attributes**, the placeholder cannot be used.

Placeholder	Description
`%a`	Returns the IP address of the service controller's Internet port.

Hosting pages on an external Web server

Use the following values to reference pages that reside on an external Web server.

Note The maximum length of any page URL is 512 characters. If this is exceeded (when using placeholders for example), the URL is truncated. Therefore, it is recommended that you specify the most-important placeholders first.

Note The service controller maintains a separate copy of the URLs for external pages for each user. This means it is possible to provide different pages for each user. See *Displaying custom welcome and goodbye pages on page 8-14*.

Welcome page

`welcome-url=URL_of_page[placeholder]`

The user is authenticated, so the welcome page can be located on any URL reachable by the user.

Login error page

`login-err-url=URL_of_page[placeholder]`

Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition. (Users can see this page *before* they are logged in.)

if the radius server denies user authentication, this is used instead of an error being presented on the login page.

Goodbye page

`goodbye-url=URL_of_page[placeholder]`

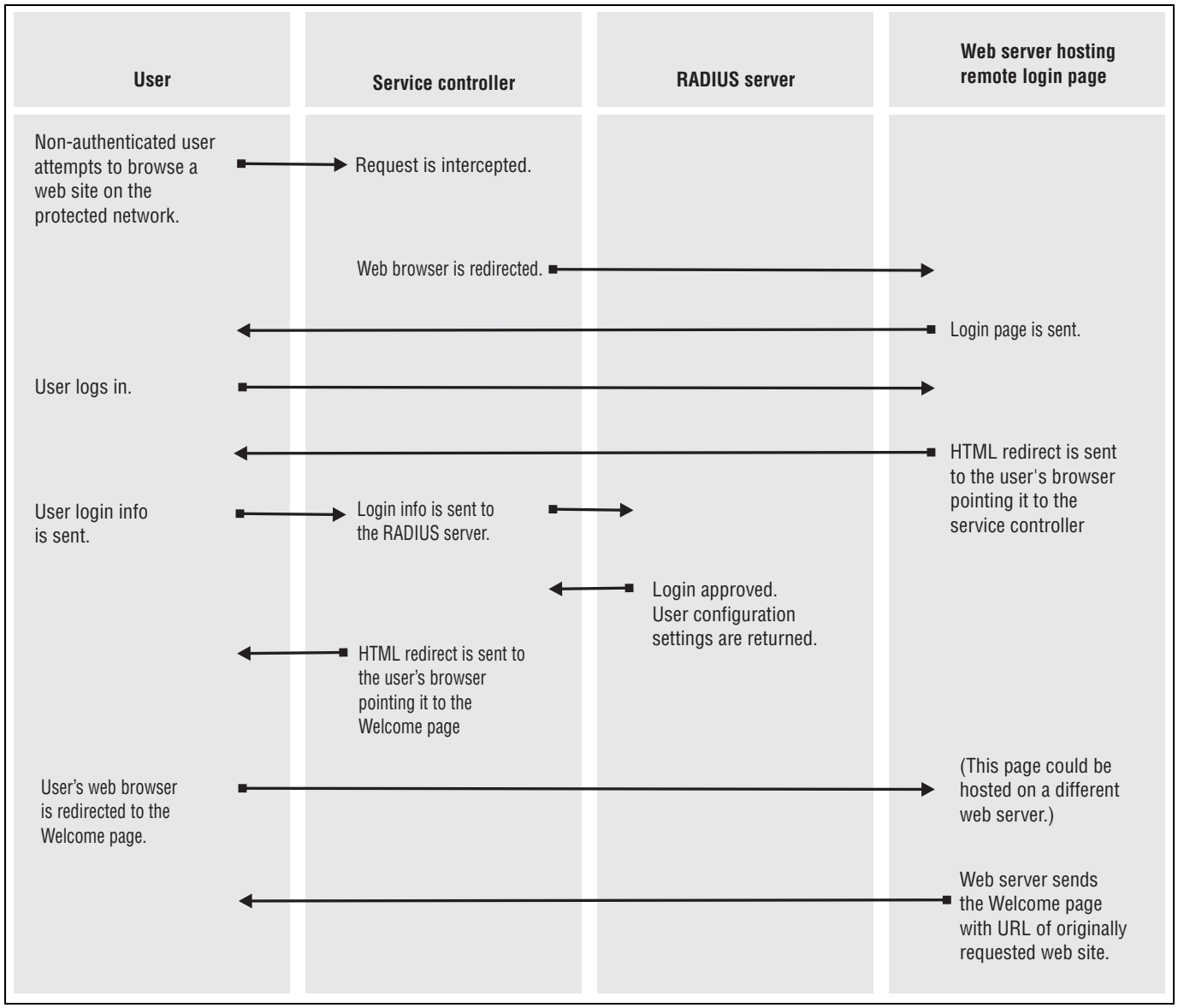
Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition. (Users see this page *after* they are logged out.)

Remote login page

Use this value to redirect users to a remote server to log in to the public access interface instead of using the internal login page.

Although the remote login page feature enables you to host the public access login page on a remote Web server, authentication of users is still performed by the service controller through a RADIUS server or using the local user list. To accomplish this, the remote Web server must send user login information back to the service controller. There are two ways this can be done: basic remote login (as described in this section), or by using the NOC-based authentication feature (described in *Appendix D: NOC authentication*).

The following diagram shows the sequence of events for a typical user session when using a remote login page and a RADIUS server for authentication.


User
Service controller
RADIUS server
Web server hosting remote login page
Non-authenticated user attempts to browse a web site on the protected network.
Request is intercepted.
Web browser is redirected.
Login page is sent.
User logs in.
HTML redirect is sent to the user's browser pointing it to the service controller
User login info is sent.
Login info is sent to the RADIUS server.
Login approved. User configuration settings are returned.
HTML redirect is sent to the user's browser pointing it to the Welcome page
User's web browser is redirected to the Welcome page.
(This page could be hosted on a different web server.)
Web server sends the Welcome page with URL of originally requested web site.

Syntax

```
login-url=URL_of_the_page [placeholder]
```

Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition. (Users see this page *before* they are logged in.)

Placeholders

An important feature of these pages is that they make it easy to deliver a unique experience for each user. By appending the following optional placeholders to the Colubris AV-Pair value strings, you can pass important information to the Web server. Server-side code can process this information to generate custom pages on-the-fly.

Placeholder	Description
`%d`	Returns the WISPr location-ID. Supported for login-url only.
`%e`	Returns the WISPr location-Name. Supported for login-url only.
`%l`	Returns the URL on the service controller where user login information should be posted for authentication. This option is used with the remote login page feature. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%n`	Returns the NAS ID assigned to the service controller. By default, this is the unit serial number. Not supported in local mode.
`%s`	Returns the RADIUS login name assigned to the service controller. By default, this is the unit serial number.
`%u`	Returns the login name of the user.
`%o`	Returns the original URL requested by the user. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%i`	Returns the domain name assigned to the service controller Internet port.
`%p`	Returns the IP port number on the service controller where user login information should be posted for authentication.
`%a`	Returns the IP address of the service controller Internet port.
`%E`	When the location-aware feature is enabled, returns the ESSID of the wireless AP the user is associated with.
`%P`	When the location-aware feature is enabled, returns the wireless mode (“ieee802.11a”, “ieee802.11b”, “ieee802.11g”) the user is using to communicate with the AP.
`%G`	When the location-aware feature is enabled, returns the group name of the wireless AP the user is associated with.
`%C`	When the location-aware feature is enabled, returns the Called-station-id content for the wireless AP the user is associated with.

Placeholder	Description
`%r`	Returns the string sent by the RADIUS server when an authentication request fails. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.
`%m`	Returns the MAC address of the client station that is being authenticated.
`%v`	Returns the VLAN assigned to the client station at the service controller ingress (LAN port).

Security issues

- It is recommended that the Web server hosting the remote login page be secured with SSL (requires an SSL certificate from a well-known certificate authority), to ensure that user logins are secure. Without SSL security, logins are exposed and may be compromised, enabling fraudulent use of the network.
- Communications between the user's browser and the service controller is always SSL-based. The default certificate on the service controller generates a warning on the user's browser unless replaced with a certificate signed by a well-known certificate authority.

Example

1. Create the following folder on your Web sever: **newlogin**.
2. See *Public access examples on page 8-4*. Copy the following sample pages into the **newlogin** folder:
   - login.html
   - transport.html
   - session.html
   - fail.html
   - logo.gif
3. Add the following entries to the **Configured attributes** table on the **Public access > Attributes** page. (You can also define these attributes in the RADIUS profile for the service controller if you are using a RADIUS server.)

```
login-url=web_server_URL/newlogin/login.html?loginurl=%l
transport-page=web_server_URL/newlogin/transport.html
session-page=web_server_URL/newlogin/session.html
fail-page=web_server_URL/newlogin/fail.html
logo=web server URL/newlogin/logo.gif
access-list=loginserver,ACCEPT,tcp,web_server_IP_address
use-access-list=loginserver
```

4. Customize **login.html** to accept username and password information from users and then send it to the service controller. You can use code similar to the following example to redirect the user's Web browser to the login URL on the service controller for authentication:

```
<form action="https://wireless.colubris.com:8090/goform/HtmlLoginRequest"
method="POST">
```

   For more flexibility, the remote login page should be written using a server-side scripting language such as ASP, PHP, or PERL. This enables the remote login page to take advantage of any placeholders that may have been defined in the login-url.

Custom message file

Use this value to load a custom message file. These messages are used when various error conditions occur.

`messages=`*URL_of_text_file* `[placeholder]`

If you specify a new message file, you must also specify values for:

- Login page
- Transport page
- Session page
- Fail page
- Logo

Placeholders
The following optional placeholder can be appended to the Colubris AV-Pair value for the message file.

Placeholder	Description
`%a`	Returns the IP address of the service controller Internet port.

Default user interim accounting update interval

This keyword lets you define the interim accounting update interval for all users that do not have a specific interval set in their profile.

Syntax

```
default-user-acct-interim-update=value
```

Where:

Parameter	Description
`value`	Number of seconds between interim updates.

Default user bandwidth level

This keyword lets you define the bandwidth level for all users that do not have a specific level set in their profile. The actual data rate associated with a bandwidth level is defined on the **Network > Bandwidth control** page.

Syntax

`bandwidth-level=`*`level`*

Where:

Parameter	Description
`level`	Specify one of the following the bandwidth levels for the user's session: VERY-HIGH HIGH NORMAL LOW

Default user idle timeout

Use this to set the default idle timeout for all users whose RADIUS profile does not contain a value for the RADIUS attribute *idle-timeout*.

Syntax

`default-user-idle-timeout=seconds`

Where:

Parameter	Description
`seconds`	Specify the maximum amount of time a user session can be idle. Once this time expires, the session is automatically terminated. A value of 0 means no timeout.

Default user quotas

These keywords let you define upload and download limits for all users that do not have a specific limit set in their profile. Limits can be defined in terms of packets or octets (bytes).

Syntax

```
default-user-max-input-packets=value
default-user-max-output-packets=value
default-user-max-total-packets=value
```

```
default-user-max-input-octets=value
default-user-max-output-octets=value
default-user-max-total-octets=value
default-user-max-input-rate=value
default-user-max-output-rate=value
```

Where:

Parameter	Description
`value`	For packets: 32-bit unsigned integer value. For octets: 64-bit unsigned integer value.

When a user session is terminated based on a quota, a new non-standard termination cause is used. The value for this termination cause is 0x8744. You can customize this by modifying the value of “radius-quota-exceeded-cause” in the “ACCESS-CONTROLLER” section of the configuration file.

The text value for the termination cause is defined in the **message.txt** file under the token “stat-quota-exceeded”. The default value for this token is “Logged out. (Quota Exceeded.)”. This value can be displayed with the ASP function GetAuthenticationErrorMessage(). See *GetAuthenticationErrorMessage() on page 9-87*.

A series of ASP functions are available that enable you to view quota information on the session page. See *Session quotas on page 9-80*.

Default user data rates

These keywords let you define data rate limits for all users that do not have a specific limit set in their profile.

Syntax

```
default-user-max-input-rate=value
default-user-max-output-rate=value
```

Where:

Parameter	Description
`value`	For packets: 32-bit unsigned integer value. For octets: 64-bit unsigned integer value.

Default user one-to-one NAT

This keyword lets you define the default setting for one-to-one NAT support for all users that do not have this setting specified in their profile. This feature only applies to users making IPSec or PPTP VPN connections with a remote site via service controller Internet port.

Syntax

```
default-user-one-to-one-nat=value
```

Where:

Parameter	Description
`value`	Set this to 1 to activate one-to-one NAT support.

Default user session timeout

Use this to set the default session timeout for all users whose RADIUS profile does not contain a value for the RADIUS attribute *session-timeout*.

Syntax

```
default-user-session-timeout=seconds
```

Where:

Parameter	Description
`seconds`	Specify the maximum amount of time a user session can be connected. Once this time expires, the session is automatically terminated. A value of 0 means no timeout.

Default user public IP address

Use this to set the default value for public IP address assignment for users whose RADIUS profile does not contain a value for **use-public-ip-subnet** (*Public IP address on page 9-66*).

Syntax

```
default-user-use-public-ip-subnet=value
```

Where:

Parameter	Description
`value`	Set this to 1 to activate assignment of a public IP address. Set to 0 to disable.

Default user SMTP server

Use this to set the default SMTP server address for all user sessions. This address is used if a specific server is not set for a particular user.

Syntax

```
default-user-smtp-redirect=hostname[:port][,username,password]
```

Where:

Parameter	Description
`hostname`	Specify the IP address or domain name of the e-mail server. Maximum length is 253 characters.
`port`	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
`username`	Specify the username required to log on to the SMTP server. Maximum 32 characters. Only used if the **SMTP authentication** option is enabled on the **Public Access > Access Control** page. Works with SMTP servers that support plain or CRAM-MD5 authentication.
`password`	Specify the password required to log on to the SMTP server. Maximum 32 characters. Only used if the **SMTP authentication** option is enabled on the **Public Access > Access Control** page. Works with SMTP servers that support plain or CRAM-MD5 authentication.

Default user URLs

Use this to set the default URLs for the welcome and goodbye pages for all users that do not have default pages specified in their profile.

Syntax

```
default-user-welcome-url=URL
default-user-goodbye-url=URL
```

Where:

Parameter	Description
`URL`	Specify the URL of an external Web page.

HTTP proxy upstream

The HTTP proxy upstream feature can be used to force all outgoing TCP traffic to be sent to a third-party upstream HTTP proxy server.

Outgoing traffic is automatically translated into HTTP proxy format because many HTTP proxies are not able to handle transparent proxy requests. HTTP requests such as GET / HTTP/1.0 are transformed into GET http://www.website.com/ HTTP/1.0 before being forwarded to the upstream server.

Note

The HTTP proxy upstream feature targets the HTTP protocol and not HTTPS. Because of this, HTTPS only works if users have configured their browsers for HTTP proxy usage. In the case of transparent proxy, the connection will not be detected as HTTP-compatible and will not be redirected to the upstream proxy server.

By default this feature listens to TCP port 8088 on the LAN port. However, it can be configured to capture other ports. This is done by defining an access list and DNAT server. For example:

```
HTTP-Proxy-Upstream=myproxy.com:8888

Access-List=mylist,DNAT-SERVER,tcp,*mydomain.com,80

Use-access-list=mylist

DNAT-Server=mylist,192.168.1.1,8088
```

This forces any traffic any incoming traffic with a target address inside **mydomain.com** to be redirected to the internal HTTP proxy. Then, because of the HTTP-Proxy-Upstream keyword, the traffic is forwarded to **myproxy.com**.

Note The HTTP-Proxy-Upstream definition must exclude any traffic addressed to the service controller public access interface, otherwise HTML-based user's will not be able to login.

Syntax

```
HTTP-Proxy-Upstream=hostname:port
```

Where:

Parameter	Description
`hostname`	Specify the IP address or domain name of the proxy server. Maximum length is 253 characters.
`port`	Specify the port on the proxy server. Range: 1 to 65535.

IPass login URL

This keyword lets you define the location of the IPass login page. The service controller will automatically redirect users with IPass client software to this page.

Syntax

```
ipass-login-url=URL_of_page
```

Where:

Parameter	Description
`URL_of_page`	Address of the IPass login page.

MAC authentication

The service controller can authenticate devices based on their MAC address. This is useful for authenticating devices that do not have a Web browser (cash registers, for example). It can also be used to authenticate an AP.

To make use of this feature you need to define a local user account or a RADIUS user account for each device as follows:

- username: Set this to the username you specified in the mac-address value string. If no username is specified, set the account name to the MAC address of the device. Use dashes to separate characters in the address. For example: 00-20-E0-6B-4B-44.
- password: Set this to the password you specified in the mac-address value string. If no password is specified, set this to the same password that is used for the user account.

Note The username and password are not encrypted for transmission so it is important that the link with the RADIUS server is secure.

Note MAC authentication only applies to VSCs that have HTML-based authentication enabled.

Syntax

```
mac-address=address[,username[,password]]
```

Where:

Parameter	Description
`address`	Specify the MAC address of the device to authenticate. Use dashes to separate characters in the address. Do not use colons (:). For example: 00-20-E0-6B-4B-44.
`username`	Specify the username to associate with this MAC address. Maximum 32 alphanumeric characters. The username field cannot contain a comma.
`password`	Specify the password to associate with this MAC address. Maximum 32 alphanumeric characters. The password field cannot contain a comma.

Example
Consider the scenario where several APs are installed with a service controller. If the APs are going to perform software updates from a remote Web or FTP server, they will need to log in to the public access network. By using MAC-based authentication, this can easily be accomplished.

Multiple login servers

This feature lets you dynamically set the URL used for retrieving custom external pages or a remote login page based on the status of a primary or secondary Web server.

Syntax

```
primary-web-server-status-url=URL_of_page

secondary-web-server-status-url=URL_of_page
```

Where:

Parameter	Description

URL_of_page	Specify the URL that points to the Web server status file. Use HTTP or HTTPS with a port number if required.
	
	The status file must contain the following code:
	
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<SOAP-ENV:Envelope`
	`  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"`
	`  xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"`
	`  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
	`  xmlns:xsd="http://www.w3.org/2001/XMLSchema"`
	`  xmlns:MYCOMPANY="http://www.mycompany.com/SOAP/NOCAPI/1.0/">`
	`  <SOAP-ENV:Body>`
	`  <MYCOMPANY:WebServerStatus>`
	`  <MYCOMPANY:result>UP</MYCOMPANY:result>`
	`  </MYCOMPANY:WebServerStatus>`
	`  </SOAP-ENV:Body>`
	`</SOAP-ENV:Envelope>`
	
	Change the `<MYCOMPANY:result>` line to indicate the status of the server as follows:
	
	Server is UP
	<MYCOMPANY:result>UP</MYCOMPANY:result>
	
	Server is DOWN
	<MYCOMPANY:result>DOWN</MYCOMPANY:result>
	
	Do not change any other lines in the file.

Polling

The service controller attempts to retrieve the server status file from the primary server first. If no response is received before the polling timeout expires (30 seconds by default), the service controller attempts to retrieve the server status file from the secondary server. If no response is received before the polling timeout expires, unauthenticated users attempting to login will see the Fail page with the message: “Login server is unavailable”.

After initialization, the service controller continuously polls the servers to determine their status. As long as the primary server is available, it is used. if the primary server fails to respond or returns status DOWN, then the secondary server will be used, but only until the primary server comes back up.

The polling interval and polling timeout are configured by editing the following entries in the configuration file: **web-server-polling-interval** and **web-server-polling-timeout.**

To change the error message, edit the entry **err-msg-login-server-down** in **messages.txt**.

Setting the URLs of other AV-Pair values

This feature will redefine the URLs in the following AV-Pair values, if they have the same hostname as is specified for the **primary-web-server-status-url**:

- login-url
- welcome-url
- goodbye-url
- logout-url
- login-err-url
- ipass-login-url

For example, if the following values are defined:

```
primary-web-server-status-url=https://srv1.abc.com/status.html
secondary-web-server-status-url=https://srv2.abc.com/status.html
login-url=https://srv1.abc.com/loginpage.html
welcome-url=http://srv1.abc.com/mywelcome.html
login-err-url=http://srv3.xyx.com/mywelcome.html
```

- If the primary server is up, then the URLs are not changed.
- If the primary server is down and the secondary server is up, then login-url and welcome-url are changed as follows:

```
login-url=https://srv2.abc.com/loginpage.html
welcome-url=http://srv2.abc.com/mywelcome.html
```

- If both servers are down, then the URLs are not changed.

Redirect URL

The redirect-url value is used to specify the target URL for redirection when using an access list with the REDIRECT action. Only one **redirect-url** value can be specified in each service controller or user RADIUS account.

When an access list rule with the REDIRECT action is processed, the user's browser is redirected to a different HTTP address in this order:

- redirect-url keyword in the user account, if present
- redirect-url keyword in the service controller account, if present
- login-url keyword, in the service controller account, if present

The URL can contain any of the applicable placeholders defined here.

Note Placeholders %G, %C, %E, %P, and %v do not produce constant values. These values may vary over time.

Use the following Colubris AV-Pair value string:

`redirect-url=`*`URL_of_the_page`* `[`*`placeholder`*`]`

Where:

Parameter	Description
URL_of_the_page	URL of the redirect page. Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition.

The following placeholders can be added to the redirect-url string.

Placeholder	Description
`%c`	Returns the IP address of the user's computer.
`%l`	Returns the URL on the service controller where user login information should be posted for authentication. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%n`	Returns the NAS ID assigned to the service controller. By default, this is the unit serial number. Not supported in local mode.
`%s`	Returns the RADIUS login name assigned to the service controller. By default, this is the unit serial number. Not supported in local mode.
`%o`	Returns the original URL requested by the user. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%i`	Returns the domain name assigned to the service controller Internet port.
`%p`	Returns the port number on the service controller where user login information should be posted to for authentication.
`%a`	Returns the IP address of the service controller interface that is sending the authentication request.
`%E`	When the location-aware feature is enabled, returns the ESSID of the wireless access point the user is associated with.
`%P`	When the location-aware feature is enabled, returns the wireless mode ("ieee802.11a", "ieee802.11b", "ieee802.11g") the user is using to communicate with the access point.

Placeholder	Description
%G	When the location-aware feature is enabled, returns the group name of the wireless access point the user is associated with.
%C	When the location-aware feature is enabled, returns the Called-station-id content for the wireless access point the user is associated with.
%r	Returns the string sent by the RADIUS server when an authentication request fails. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.
%m	Returns the MAC address of the wireless/wired client station that is being authenticated.
%v	Returns the VLAN assigned to the client station at the service controller ingress (LAN port).

Note The maximum length of the remote login page URL is 512 characters. If this is exceeded (when using placeholders for example), the URL is truncated. It is therefore recommended that you specify the most-important placeholders first.

Example

One way to use this feature is to offer a premium service for a given (or all) sites. For example, in the service controller profile, define two lists, one for normal usage and one for premium usage:

```
access-list=normal,REDIRECT,tcp,www.mypremiumservice.com,80
access-list=normal,ACCEPT,all,all,all
access-list=premium,ACCEPT,all,all,all
redirect-url=http://www.mysite.com/getpremium/
```

In the RADIUS profile for normal users, map them to the “normal” access list:

```
use-access-list=normal
```

In the RADIUS profile for premium users, map them to the “premium” access list:

```
use-access-list=premium
```

The access list only takes effect on an authentication, so a change of service as shown in this example takes effect only at the user’s next authentication (login).

NOC authentication

The NOC authentication feature provides a secure way of authenticating public access users, with strong mutual authentication between the login application on the Web server hosting the remote login page and the service controller used for authenticating user logins. This occurs via the two Colubris AV-Pair value strings (**ssl-noc-certificate** and **ssl-noc-ca-certificate**), which define the locations of two certificates. These certificates enable the service controller to validate that the user login information does indeed come from a trusted application.

For example, from a login application on the Web server.

`ssl-noc-certificate=URL_of_the_certificate`

Certificate issued to the application on the Web server that will send user info to the service controller for authentication.

`ssl-noc-ca-certificate=URL_of_the_certificate`

Certificate of the certificate authority (CA) that issued the NOC certificate.

For a more detailed example of using NOC authentication, see *Appendix D: NOC authentication*

ProCurve WISPr support

WISPr login URL

This keyword lets you define the location of the WISPr login page. The service controller automatically redirects users with WISPr-compatible wireless client software to this page. To customize the redirection use the WISPr redirect page keyword.

Syntax

`wispr-login-url=URL_of_page`

Where:

Parameter	Description
`URL_of_page`	URL of the WISPr login page.

WISPr abort login URL

This keyword lets you define the destination where the WISPr abort login will be POSTed.

Syntax

`wispr-abort-login-url=URL_of_page`

Where:

Parameter	Description
`URL_of_page`	URL where to POST the WISPr abort login.

WISPr redirect page

This keyword lets you define the location of the WISPr redirect page. Use this page to customize the code that the service controller includes in the HTTP redirect sent to a user's browser.

Syntax

```
redirect-page=URL_of_page
```

Where:

Parameter	Description
`URL_of_page`	URL of the page containing code to use for WISPr redirect.

If this keyword is not defined, default code is used. To view the default code, open the file **redirect.html** which is available in the Public Access Examples file. See *Public access examples on page 8-4*.

WISPr access procedure

Specifies the version of the WISPr client access procedure supported by the service controller.

```
access-procedure=procedure_version
```

Where:

Parameter	Description
`procedure_version`	Specify the WISPr client access procedure supported by the service controller. Currently, the service controller only supports the value "1.0".

Traffic forwarding (dnat-server)

This keyword defines the external server to which the service controller will forward traffic when an access list rule with the DNAT-SERVER action matches incoming traffic.

Two external servers can be defined with this keyword. A status polling mechanism is available that enables the service controller to determine the status of the external servers and forward traffic to the one this is operational. To activate the polling mechanism see *Multiple DNAT servers* below.

This keyword can be defined directly on the service controller or in the service controller RADIUS profile.

Syntax

```
dnat-server=listname,hostname,port[,hostname2,port2]
```

Where:

Parameter	Description
`listname`	Specify the name of an access list definition that has its action set to DNAT-SERVER.
`hostname`	Specify the IP address or domain name of the primary server to which traffic will be redirected. Maximum length is 253 characters. If polling is not enabled, traffic is always sent to this server, even if it is down.
`port`	Specify the port on the primary server to which traffic will be redirected. Range: 1 to 65535.
`hostname2`	Specify the IP address or domain name of the secondary server to which traffic will be redirected. Maximum length is 253 characters. Traffic will only be sent to the secondary server if polling is enabled and the primary server is down. See *Multiple DNAT servers on page 9-61*.
`port2`	Specify the port on the secondary server to which traffic will be redirected. Range: 1 to 65535.

Example

The following creates an access list called **redirect** which is used to redirect HTTP traffic for authenticated users to **server1.mycompany.com** on port **8080**.

The following entry is added to the local profile for the service controller:

```
access-list=redirect,DNAT-SERVER,tcp,all,80
```

```
dnat-server=redirect,srv1.mycompany.com,8080
```

Multiple DNAT servers

The **dnat-server** keyword supports the definition of two external servers. To make use of these servers a polling mechanism is provided. Two keywords are available to activate and configure the polling mechanism.

Syntax

```
primary-dnat-server-status-url=listname,URL_of_page
```

```
secondary-dnat-server-status-url=listname,URL_of_page
```

Where:

Parameter	Description
`listname`	Specify the name of an access list definition that has its action set to DNAT-SERVER.

`URL_of_page`	Specify the URL that points to a status file on the Web server. Use HTTP or HTTPS with a port number if required.
	
	The status file must contain the following code:
	
	`<?xml version="1.0" encoding="UTF-8"?>`
	`<SOAP-ENV:Envelope`
	`  xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/"`
	`  xmlns:SOAP-ENC="http://schemas.xmlsoap.org/soap/encoding/"`
	`  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"`
	`  xmlns:xsd="http://www.w3.org/2001/XMLSchema"`
	`  xmlns:MYCOMPANY="http://www.mycompany.com/SOAP/NOCAPI/1.0/">`
	`  <SOAP-ENV:Body>`
	`  <MYCOMPANY:WebServerStatus>`
	`  <MYCOMPANY:result>UP</MYCOMPANY:result> <!- Change this between UP and DOWN to determine the state of your server !>`
	`  </MYCOMPANY:WebServerStatus>`
	`  </SOAP-ENV:Body>`
	`</SOAP-ENV:Envelope>`
	
	Change the `<MYCOMPANY:result>` line to indicate the status of the server as follows:
	
	Server is UP
	<MYCOMPANY:result>UP</MYCOMPANY:result>
	
	Server is DOWN
	<MYCOMPANY:result>DOWN</MYCOMPANY:result>
	
	Do not change any other lines in the file.
	
	If the service controller fails to receive an answer to a poll, or receives an incorrect answer (bad format, wrong result setting) it is interpreted as the server being down.

Polling

Initially, the service controller polls the primary server at an interval of 10 minutes. As long as the primary is active, it is used. If it is not available, then the secondary server is used, but only until the primary server becomes available again.

If both servers are not available, both are polled in turn with no delay (other than the poll timeout) until one becomes available. When both servers are unavailable the access list DNAT-SERVER definition is skipped with no action taken, and processing moves to the next rule in the access list. This next rule can then be used to define the action taken when both DNAT-SERVERS are down.

The following table shows possible results when polling is active for both the primary and secondary servers.

Server 1	Server 2	Description
UP	UP	Traffic matching the DNAT-SERVER rule is forwarded to server 1.
UP	DOWN	Traffic matching the DNAT-SERVER rule is forwarded to server 1.
DOWN	UP	Traffic matching the DNAT-SERVER rule is forwarded to server 2.
DOWN	DOWN	No action is performed for the DNAT-SERVER rule. Processing moves to the next rule in the list. To accept all traffic if both servers are down, define this rule as: ACCEPT,all,all,all

Example

The following creates an access list called **redirect** which is used to redirect HTTP traffic for authenticated users to either **srv1.mycompany.com** or **srv2.mycompany.com** depending on which one is active. Port **8080** is used to forward traffic. If neither the primary or secondary DNAT-SERVER is available, all traffic is accepted.

The following entry is added to the local profile for the service controller:

```
access-list=redirect,DNAT-SERVER,tcp,all,80
```

```
access-list=redirect,ACCEPT,all,all,all
```

The following entry is added to the RADIUS profile for each user:

```
dnat-
server=redirect,srv1.mycompany.com,8080,srv2.mycompany.com,8080
```

Colubris AV-Pair attribute - User values

User values let you define settings for individual user accounts.

Each Colubris AV-Pair value is specified using the following format: `<keyword>=<value>`

The following table lists all supported user value keywords and provides a link to complete descriptions for each one.

Colubris AV-Pair keyword	For more information see
access-list	*Access list on page 9-64.*
ads-presentation	*Advertising on page 9-65.*
bandwidth-level	*Bandwidth level on page 9-65.*
max-output-rate max-input-rate	*Data rate on page 9-65.*
one-to-one-nat	*One-to-one NAT on page 9-66.*
use-public-ip-subnet	*Public IP address on page 9-66.*
max-input-packets max-output-packets max-input-octets max-output-octets max-total-octets max-total-packets	*Quotas on page 9-66.*
smtp-redirect	*SMTP redirection on page 9-67.*
polling-arp-interval polling-max-arp-count	*Station polling on page 9-68.*
redirect-url	*Colubris AV-Pair attribute - Administrator values on page 9-69.*

Access list

An access list is a set of rules that govern how the service controller controls user access to protected network resources (those attached to the service controller Internet port). Access lists are defined in the profile for the service controller) and are activated in user profiles as needed.

Only one access list can be activated per user profile. See *Access list on page 9-30*.

Syntax

`use-access-list=`*`uselistname`*

Where:

Parameter	Description
`uselistname`	Specify the name of an existing access list. This list is activated for the current user.

Advertising

Add this keyword to enable the presentation of advertising at preconfigured intervals while the user is browsing.

Syntax

ads-presentation=*value*

Where:

Parameter	Description
value	Set this to 1 to activate the display of advertising. Set to 0 to disable.

Bandwidth level

This keyword sets bandwidth level for a user's session. The actual data rate associated with a bandwidth level is defined on the **Network > Bandwidth control** page.

Syntax

bandwidth-level=*level*

Where:

Parameter	Description
level	Specify one of the following the bandwidth levels for the user's session: VERY-HIGH HIGH NORMAL LOW

Data rate

This keyword sets the transmit and receive rates for a user's session. These rates are applied on a per-user basis providing direct control of a user's throughput in Kbps. Two keywords are available:

- max-input-rate: Controls the data rate at which traffic can be transferred from the user to the service controller.
- max-output-rate: Controls the data rate at which traffic can be transferred from the service controller to the user.

Note The settings for bandwidth level always take precedence over user data rates. This means if you set a data rate which exceeds the configured bandwidth level, the rate is capped at the bandwidth level.

Syntax

`max-output-rate=`*`rate`*
`max-input-rate=`*`rate`*

Where:

Parameter	Description
`rate`	Maximum transmit or receive speed in Kbps.

One-to-one NAT

Note This feature only applies to client traffic using IPSec or PPTP on the Internet port.

Add this keyword if the user requires a unique IP address when NAT is enabled on the service controller.

Syntax

`one-to-one-nat=`*`value`*

Where:

Parameter	Description
`value`	Set this to 1 to activate one-to-one NAT support.

Public IP address

Add this keyword if the user requires a public IP address that is visible on the external network connected to the service controller Internet port.

Syntax

`use-public-ip-subnet=`*`value`*

Where:

Parameter	Description
`value`	Set this to 1 to activate assignment of a public IP address. Set to 0 to disable.

Quotas

These keywords let you define upload and download limits for each user. Limits can be defined in terms of packets or octets (bytes).

Syntax

```
max-input-packets=value
max-output-packets=value
max-input-octets=value
max-output-octets=value
max-total-octets=value
max-total-packets=value
```

Where:

Parameter	Description
`value`	For packets: 32-bit unsigned integer value. For octets: 64-bit unsigned integer value.

When a user session is terminated based on a quota, a new non-standard termination cause is used. The value for this termination cause is 0x8744. The text value of for the termination cause is defined in the message.txt file under the token “stat-quota-exceeded”. The default value for this token is “Logged out. (Quota Exceeded.)”. This value can be displayed with the ASP function *GetAuthenticationErrorMessage() on page 9-87*

A series of ASP functions are available that enable you to display quota information on the session page. See *Session quotas on page 9-80*.

Redirect URL

The redirect-url keyword is used to specify the target URL for redirection when using an access list with the REDIRECT action. Only one **redirect-url** value can be specified in a user RADIUS account. See *Redirect URL on page 9-56*.

SMTP redirection

The service controller is able to provide SMTP email service on a per-user basis. This enables users to send e-mail while on the road without the restrictions imposed by most ISPs regarding the source address of outgoing mail. It works by intercepting the call to a user’s e-mail server and redirecting it to an SMTP server that you configure. This setting overrides the setting of *Default user SMTP server on page 9-51*.

Note For mail redirection to work, the user's email server name must be publicly known. If the e-mail server name cannot be resolved, mail redirection fails.

Note If an access list definition is active in the service controller profile that enables unauthenticated users to access their SMTP servers, the SMTP redirect feature will not work for these users.

Syntax

```
smtp-redirect=address[:port][,username,password]
```

Where:

Parameter	Description
`address`	Specify the IP address or domain name of the e-mail server which is used to send outgoing redirected mail.
`port`	Specify the port on the e-mail server to relay to. Range: 1 to 65535. Default: 25
`username`	Specify the username required to log on to the SMTP server. Maximum 32 characters. Only supported if the **Support authentication on SMTP proxy server** option is enabled on the **Public access > Access control** page. Works with SMTP servers that support PLAIN, CRAM-MD5, and no authentication.
`password`	Specify the password required to log on to the SMTP server. Maximum 32 characters. Only supported if the **Support authentication on SMTP proxy server** option is enabled on the **Public access > Access control** page. Works with SMTP servers that support PLAIN, CRAM-MD5, and no authentication.

Example 1: Proxy support on

```
smtp-redirect=smtp.mycompany.com,jimmy,letMEin
smtp-redirect=smtp.mycompany.com:8025,jimmy,letMEin
```

Example 2: Proxy support off

```
smtp-redirect=smtp.mycompany.com
smtp-redirect=smtp.mycompany.com:8025
```

Station polling

The service controller continually polls authenticated client stations to ensure they are active. This feature is configured using the **Client polling** settings on the **Public access > Access control** page. If no response is received and the number of retries is reached, the client station is disconnected.

These keywords let you override the **Client polling** settings on a per-user basis.

Syntax

`polling-arp-interval=`*`interval`*

`polling-max-arp-count=`*`count`*

Where:

Parameter	Description
`interval`	Specify how (in seconds) long to wait between polls.

Parameter	Description
`count`	Specify how many polls a client station can fail to reply to before it is disconnected.

To disable polling, set both *interval* and *count* to 0.

The initial query is always done after the client station has been idle for 60 seconds. If there is no answer to this query, the settings for polling-arp-interval and polling-max-arp-count are used to control additional retries.

Colubris AV-Pair attribute - Administrator values

Administrator values let you define settings for administrator accounts.

Each Colubris AV-Pair value is specified using the following format: `<keyword>=<value>`

The following administrator value keyword is supported:

Administrative role

Use this AV-Pair value to identify the role of administrative accounts. See also, *Management tool on page 4-2*.

Syntax

`web-administrative-role=role`

Where:

Parameter	Description
`role`	Use one of the following values to identify the role of the account: ■ **Manager:** A manager is able to access all configuration pages and can change and save all configuration settings. ■ **Operator:** An operator is able to view all configuration pages, but is limited in the types of changes that can be made.

Public access interface ASP functions and variables

The public access interface Web pages use a number of ASP functions to perform specific tasks. These ASP functions are written in embedded Javascript, which is a limited version of Javascript running on the integrated Web server.

Also, a number of ASP variables are defined that can be used to store and retrieve configuration and user settings. There are two types of variables”

- **ASP variables:** The values of these variables must be loaded before they can be used by calling the appropriate ASP function. Values are only persistent per page. Therefore they must be loaded separately on each page before use.
- **Session variables:** Session variables are persistent across all public access pages.

Javascript syntax

The following syntax is used by embedded Javascript code.

Equality and relational operators

	Syntax	Description
Equality operators	==	Equal to
	!=	Not equal to
	>	Greater than
	>=	Greater than or equal to
	<	Less than
	<=	Less than or equal to
Conditional operators	&&	Conditional And
	||	Conditional Or
Unary operator	!	Not (Inverts the value of a boolean value.)
String operator	+	Concatenates two strings.
Arithmetic operators	+	Addition.
	-	Subtraction.
	/	Division.
	*	Multiplication.
	( )	Priority of evaluation.
Control flow	if (*logical condition*) {} else {}	If then else statement.
	for(start; until; steps) { }	Looping.

Forms

The following forms can be used to gather information from a user and submit it to the public access interface for processing.

HtmlSubscriptionRequest

This form can be used create a user account and to execute a payment.

To complete certain form actions, you may be required to submit several parameters. These parameters do not all have to be submitted at the same time. The public access interface will combine the values from multiple POSTs and execute the required task once all required data has been submitted. This allows tasks that require many user inputs (creation of a new account, for example) to be spread out over multiple pages.

Before submitting this form you should clear any variable which may still be present in the session store as follows:

- ClearSessionVar(subscription_plan)
- ClearSessionVar(payment_method)
- ClearSessionVar(password)
- ClearSessionVar(card_number)
- ClearSessionVar(card_expiration)
- ClearSessionVar(cart_id)

Fields

- **cancel:** Redirects the user to **cancel_url**.
- **cancel_url:** URL to which the user is redirected when the **cancel** field is specified.
- **card_expiration:** Credit Card expiration in the format **mm/yy**.
- **card_number:** Credit Card number.
- **confirm_password:** Password of the user account.
- **error_url:** URL to which the user is redirected if an error occurs.
- **password:** Password of the user account.
- **pay:** Include this field (with any value) to execute a payment.
- **payment_method:** Payment method must be **"**CreditCard**"**.
- **subscription_plan:** Name of the subscription plan.
- **success_url:** URL to which the user is redirected if no error occurs.
- **username:** Username of the user account.
- **valid_fields:** Specify the names of the fields that should be validated. Separate field names with a space. For example: valid_fields "username password confirm_password".

To create an account

Supply to following fields to create a new user account, or to reset an existing account:

- payment_method
- subscription_plan
- username
- password
- confirm_password
- valid_fields (listing all supplied fields) For example: valid_fields "payment_method subscription_plan username password confirm_password"

To execute a payment

Supply to following fields to execute a payment:

- payment_method
- subscription_plan
- username
- password
- confirmation_password
- card_expiration
- card_number
- pay
- valid_fields (listing all supplied fields) For example:
  valid_fields “payment_method subscription_plan username password confirm_password card_expiration card_number”

Note To review payment settings, omit the pay field.

HtmlLoginRequest

This form can be used to perform several login-related actions.

Fields

- **access_type:** Determines the type of action that will be executed:
  - **login:** The **username** and **password** are used to attempt an HTML login. If the login is successful, the user is redirected to the page specified by **success_url.** If the login fails, the user is redirected to the page specified by **error_url.**
  - **subscribe:** The user is redirected to the page specified by **subscription_url**.
  - **free_access:** A user account is created (with the user’s MAC address as the username and password) and the user is logged into the public access interface. If the login is successful, the user is redirected to the page specified by **success_url.** If the login is fails, the user is redirected to the page specified by **error_url.**
- **error_url:** The URL to which the user is sent if the login fails. Applies to access_type = login or free_access.
- **original_url:** The URL that the user came from. Normally initialized using GetOriginalURL();
- **password:** Password to use for authentication. Applies to access_type = login.
- **subscription_url:** The URL to which the user is sent when access_type = subscribe.
- **success_url:** The URL to which the user is sent if the login is successful. Applies to access_type = login or free_access.

- **username:** Username to use for authentication. Applies to access_type = login.
- **valid_fields:** Name of the form fields to do validation upon.

HtmlLogout

This form performs a logout operation.

Field

- success_url: The URL to which the user is sent if the logout is successful.

Form errors

When the Web server validates a form, it builds a list of all fields that have validation errors. The following functions can be used to scan this list and retrieve error information for each field.

GetLastFormSubmitFirstField()

Returns the name of the first field (as a string) that generated a validation error. If no error occurred for any fields in the form, an empty string is returned.

Example
var firstField = GetLastFormSubmitFirstField();

GetLastFormSubmitNextField(*field_name*)

Returns the name of the next field after the specified ***field_name*** that generated an error. This enables you to move through the field error list one field at a time.

The field name is returned as a string. If no error occurred for any other fields in the form, an empty string is returned.

Example
var nextField = GetLastFormSubmitNextField("previousField");

LoadFormFieldError(*field_name*)

This function the following ASP variables with details about the errors caused by the specified ***field_name***.

ASP variables

- **field_error:** Numeric error value.
  - 0 - No error found.
  - 1 - The field required a value but was empty.
  - 2 - The field contained a value which exceeds the maximum supported length.
  - 3 - The field contained a value which is invalid (only specific values were allowed).

- **field_error_details:** Additional information about the error. Will contain an empty string if not applicable. When **field_error** is set to 2, **field_error_details** will be equal to the maximum supported field length.

Example

```
LoadFormFieldError("field");
write(field_error);
write(field_error_details);
```

RADIUS

GetMsChapV2Failed()

Displays the MS CHAP V2 error string received in the last RADIUS Reject or RADIUS Accept packet for the user. This function is only supported if you select MSCHAP V2 as the authentication scheme on the service controller (**Service Controller >> Authentication > RADIUS profiles** page). The RADIUS server must also support this feature. For a list of possible return values see RFC 2759.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetRadiusNasId()

Returns the NAS ID configured for RADIUS Profile on the service controller. This can be used to identify the service controller that authenticated a user. For an example of how this function is used, see GetNasAddress().

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetRadiusReplyMessage()

Displays the reply message content received inside the last RADIUS Request or RADIUS Accept packet for the user. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetNasAddress()

Returns the fully-qualified domain name of the service controller as is specified in the currently loaded SSL certificate.

For example, in certain instances you may want users to register for an account before they log in. To accomplish this you could modify the Login page by adding a register button. This redirects the user's browser to a registration Web server where they can set up their account. (This page must be made accessible to non-authenticated users using the appropriate access list rule.)

To avoid having the user login once registration is complete, the registration Web server can send the user back to the service controller using a special URL that automatically logs the user into the public access interface.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

Example
Assuming the registration server is 192.169.30.1, the register button code on the Login page might look something like this:

```
<FORM><INPUT
onclick="javascript:window.location='https://192.168.30.1/demo-php/
register.php?
NASip=<%GetNasAddress();%>&NASid=<%GetRadiusNasId();%>';"
type=button value="Click Here to Register">
</FORM>
```

The NAS ID and NAS address are required when the user is redirected back to the service controller after registration. The code on the registration Web page would look something like this:

```
// Registering user information in the backend database
RegisterUser($username,
$firstname,
$lastname,
$company,
$title,
$phone,
$email,
$NASid,   // identifies the service controller the user is connected to
$NASip
);

// set URL to redirect browser to
$targetURL = "location: https://
" . $NASip . ":8090/goform/HtmlLoginRequest?
username=" . $username . "&password=" . $password;

// When done
header($targetURL);
```

The target URL is built using the NAS IP and username and password. The form name is hard-coded.

Page URLs

GetFailRetryUrl()

Returns the URL of the next internal page to display as follows:

- Returns the Fail page URL if a login or logout request is currently pending.
- Returns the Transport page URL if the user is already logged in.

This function is designed to be used in conjunction with IsRequestPending().

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetLoginUrl()

Returns the URL of the Login page.

This is not a normal return value, it cannot be assigned to an ASP variable, it is inserted directly into the HTML page.

GetOriginalUrl()

Displays the URL the user tried to access before being redirected to the Login page.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetSessionUrl()

Returns the URL of the Session page.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

GetWelcomeUrl()

Returns the URL of the Welcome page.

This is not a normal return value. It cannot be assigned to an ASP variable, and is inserted directly into the HTML page.

Session status and properties

All functions in this section do not provide a normal return value that can be assigned to an ASP variable. Instead, the return value is inserted directly into the HTML page.

Session time

GetSessionStateMessage()

Returns a message (from message.txt) indicating the status of the user session.

GetSessionTime()

Returns session duration for the current user in minutes and seconds in the format: mm:ss.

ConvertSessionTime(unit)

Returns session duration for the current user in the specified unit. See *ConvertMaxSessionTime(unit) on page 9-78*.

TruncateSessionTime(unit)

Returns session duration for the current user truncated to the specified unit. See *TruncateMaxSessionTime(unit) on page 9-79*.

GetSessionTimeHMS()

Returns session duration for the current user in hours, minutes and seconds in the format: hh:mm:ss.

GetSessionRemainingTime()

Returns the amount of connection time remaining for the current user session in minutes and seconds in the format: mm:ss.

GetSessionRemainingTimeHMS()

Returns the amount of connection time remaining for the current user session in hours, minutes and seconds in the format: hh:mm:ss.

ConvertSessionRemainingTime(unit)

Returns the total amount of connection time remaining for the current user in the specified unit. See *ConvertMaxSessionTime(unit) on page 9-78*.

TruncateSessionRemainingTime(unit)

Returns the total amount of connection time remaining for the current user truncated to the specified unit. See *TruncateMaxSessionTime(unit) on page 9-79*.

GetMaxSessionTime()

Returns the total amount of connection time configured for the current user session in minutes and seconds in the format: mm:ss.

GetMaxSessionTimeHMS()

Returns the total amount of connection time configured for the current user session in hours, minutes and seconds in the format: hh:mm:ss.

ConvertMaxSessionTime(unit)

Returns the total amount of connection time configured for the current user in the specified unit.

y	Years
d	Days
h	Hours
m	Minutes
s	Seconds

For example if the user account is configured for 5000 seconds, then:

- ConvertMaxSessionTime(“y”) returns 0, calculated as (5000 / (365*24 *60*60)).
- ConvertMaxSessionTime(“d”) returns 0, calculated as (5000 / (24*60*60)).
- ConvertMaxSessionTime(“h”) returns 1, calculated as (5000 / (60*60)).
- ConvertMaxSessionTime(“m”) returns 83, calculated as (5000 / 60).
- ConvertMaxSessionTime(“s”) returns 5000, calculated as (5000 / 1).

TruncateMaxSessionTime(unit)

Returns the total amount of connection time configured for the current user truncated to the specified unit.

y	Years
d	Days
h	Hours
m	Minutes
s	Seconds

For example if the user account is configured for 5000 seconds, then:

- TruncateSessionTime("y") returns 0.
- TruncateSessionTime("d") returns 0.
- TruncateSessionTime("h") returns 1.
- TruncateSessionTime("m") returns 23.
- TruncateSessionTime("s") returns 20.

Session input/output/totals

If you specify a value for the optional parameter **div**, then the return value is divided by **div**.

GetSessionInputPackets()
GetSessionInputOctets(div)

Returns the number of packets/octets received by the current user session.

GetSessionOutputPackets()
GetSessionOutputOctets(div)

Returns the number of packets/octets sent by the current user session.

GetSessionTotalPackets()
GetSessionTotalOctets(div)

Returns the number of packets/octets sent and received by the current user session.

GetSessionMaxTotalPackets()
GetSessionMaxTotalOctets(div)

Returns the maximum number of packets/octets that can be sent and received by the current user session.

GetSessionRemainingInputPackets()
GetSessionRemainingInputOctets(div)

Returns the remaining number of packets/octets that can be received by the current user session.

GetSessionRemainingOutputPackets()
GetSessionRemainingOutputOctets(div)

Returns the remaining number of packets/octets that can be sent by the current user session.

GetSessionRemainingTotalPackets()
GetSessionRemainingTotalOctets(div)

Returns the remaining number of packets/octets that can be sent or received by the current user session.

GetSessionMaxInputPackets()
GetSessionMaxInputOctets(div)

Returns the maximum number of packets/octets that can be received by the current user session.

GetSessionMaxOutputPackets()
GetSessionMaxOutputOctets(div)

Returns the maximum number of packets/octets that can be sent by the current user session.

Session quotas

These functions let you retrieve the quota limits that are set for the current user session. If any of these limits are reached, the user is logged out. See *Quotas on page 9-66*.

If you specify a value for the optional parameter **div**, then the return value is the number of octets divided by **div**.

- Packets values are returned as a decimal string (10 characters) representing a 32-bit unsigned integer.

- Octet values are returned as a decimal string (20 characters) representing a 64-bit unsigned integer.

GetSessionRemainingInputPackets()
GetSessionRemainingInputOctets(div)

Returns the number of incoming packets/octets the current user session can still receive.

GetSessionRemainingOutputPackets()
GetSessionRemainingOutputOctets(div)

Returns the maximum number of outgoing packets/octets the current user session can still send.

GetMaxSessionInputPackets()
GetMaxSessionInputOctets(div)

Returns the maximum number of incoming packets/octets the current user session can receive.

Returns the maximum number of incoming octets the current user session can receive.

GetMaxSessionOutputPackets()
GetMaxSessionOutputOctets(div)

Returns the maximum number of outgoing packets/octets the current user session can send.

iPass support

iPassGetLoginUrl()

Returns the iPass Login URL.

iPassGetAbortLoginUrl()

Returns the iPass Abort Login URL.

iPassGetLogoffUrl()

Returns the iPass Logout URL.

iPassGetRedirectResponseCode()

Checks if the iPass authentication server is reachable and enabled. Returns one of the following values:

0	Authentication server is reachable and enabled.
105	The authentication server could not be reached or is unavailable.

255	The authentication server could not be reached due to an error on the service controller (Internet port not up, for example).

iPassGetAccessProcedure()

Returns the access procedure supported by the service controller. The service controller supports procedure version 1.0.

iPassGetLocationName()

Returns the location ID defined on the **Public access > Access control** page.

iPassGetAccessLocation()

Returns a value which can be used to determine the access point a user is connected to. This is useful when you are using one or more APs in addition to the service controller.

- If a user logs into a AP, this function returns the MAC address of the AP's downstream port.
- If a user logs into the service controller, this function returns the MAC address of the service controller LAN port.

iPassGetLoginResponseCode()

Returns one of the following values when a user attempts to login to iPass:

50	Login was successful.
100	Login failed. Access was rejected.
102	Login failed. Authentication server error or timeout.
201	Authentication is pending.
255	The authentication server could not be reached due to an error on the service controller (Internet port not up, for example).

iPassGetLogoutResponseCode()

Returns one of the following values when a user attempts to logout from iPass:

150	Logout was successful.
255	The authentication server could not be reached due to an error on the service controller (Internet port not up, for example).

Web

GetWebFullURL("http" | "https")

This function returns the full URL (protocol, hostname and port) to the root of the Web server as either HTTP or HTTPS.

Example
var url = GetWebFullURL("http");

GetHTTPProtocol()

Returns the protocol used when requesting the current Web page as a string. Possible values are:

- http
- https

Example
var protocol = GetHTTPProtocol();
write(protocol); /* will write either "http" or "https" depending on the URL you typed to view the page. */

Client information

LoadClientInformation()

This function initializes a set of variables that provide information on the user that is requesting the current page.

ASP variables

- **client_username:** String containing the username of the user if known.
- **client_useraccount_index:** String that uniquely identifies the user's account.
- **client_ip_address:** String containing the IP address of the user that requested the page.
- **client_state:** The user's authentication state: **1** for authenticated, **0** otherwise If 0, all other variables will contain their last value, unless the user was never authenticated, in which case they will be blank.
- **client_session_time:** The user's session time, indicating how many seconds have elapse since the user was first authenticated by the service controller. Re-authentication will not affect the value unless the authentication was terminated.
- **client_session_idle_time:** Indicates how many seconds have elapsed since the service controller first received traffic from this user that was inside the user's defined access-list destination(s).
- **client_session_transmitted_packets:** Number of packets the user has transmitted to destinations inside the user's defined access-list destination(s).

- **client_session_transmitted_bytes:** Number of bytes the user has transmitted to destinations inside the user's defined access-list destination(s).
- **client_session_received_packets:** Number of packets the user has received from sources inside the user's defined access-list destination(s).
- **client_session_received_bytes:** Number of bytes the user has received from sources inside the user's defined access-list destination(s).
- **client_subscription_plan_index:** The subscription plan index with which the user account is associated. A value of **0** indicates that the user account is not associated with a plan.
- **client_authentication_mode:** Indicates how the user was authenticated:

  0 - Unknown, authentication may be pending or the user is not authenticated.

  1 - Authenticated using the local user accounts.

  2 - Authenticated using a third-party RADIUS server.

  3 - Authenticated using Active Directory.
- **client_subscription_plan_name:** Name of the subscription plan assigned to the user. Additional information can be obtained using the function LoadSubscriptionPlanInformation().
- **client_subscription_plan_state:** User's subscription plan state:

  0 - Plan is invalid, expired or no plan exists for that client.

  1 - Plan is valid.
- **client_ads_presentation:** User's advertisement presentation state.

  0 - Advertisements are enabled for the user.

  1 - Advertisements are displayed for the user.
- **client_public_ip**: Indicates if the user's IP address is public or private.

  0 - IP address is private.

  1 - IP address is public.
- **client_public_ip_reserved:** Indicates if the public IP is reserved or preferred.

  0 - Public IP is preferred.

  1 - Public IP is reserved.

LoadClientAccountStatusInformation()

This function initializes a set of variables that provide information on the current user.

ASP variables

- **client_account_status_is_online_time_exhausted**: Set to **1** if online time has been exhausted.

- **client_account_status_is_time_since_first_login_expired**: Set to **1** if time since first login has been exceeded its configured limit.
- **client_account_status_is_time_currently_outside_valid_period_of_day**: Set to **1** if the current time is outside the valid period for the account.
- **client_account_status_is_validity_period_not_begun**: Set to **1** if the validity period for the account has not yet begun.
- **client_account_status_is_validity_period_ended**: Set to **1** if the validity period for the account has ended.
- **client_account_status_is_input_octets_quota_exhausted**: Set to **1** if the download limit for the account has been exhausted.
- **client_account_status_is_output_octets_quota_exhausted**: Set to **1** if the upload limit for the account has been exhausted.
- **client_account_status_is_total_octets_quota_exhausted**: Set to **1** if the total traffic quota for the account has been exceeded.
- **client_account_status_first_login_time**: Time the user first logged in.
- **client_account_status_time_since_first_login**: Elapsed time since the user first logged in.
- **client_account_status_remaining_online_time**: Amount of online time remaining.
- **client_account_status_remaining_session_time**: Amount of time remaining for which the account is still valid.
- **client_account_status_expiration_time**: Date/time at which the account will expire. This is set by determining the first Validity period rule (*Defining subscription plans on page 7-13*) that will be reached, excluding the rules that apply to time limits during a day.
- **client_account_status_remaining_input_octets**: Amount of traffic the user can still download.
- **client_account_status_remaining_output_octets**: Amount of traffic the user can still upload.
- **client_account_status_remaining_total_octets**: Total amount of traffic the user can still upload or download.
- **client_account_status_active_sessions**: Number of sessions active on this account.

Subscription plan information

LoadSubscriptionPlanInformation(*subscription_plan*)

This function initializes a set of variables that provide information on the specified subscription plan.

ASP variables

- **subscription_plan_name:** Name of the plan.

- **subscription_plan_id:** ID which uniquely identifies each subscription plan.
- **subscription_plan_fee:** Subscription plan cost.
- **subscription_plan_tax:** Subscription plan tax. Calculated based on the subscription plan cost and the configured tax rate.
- **subscription_plan_total:** Total subscription plan charge.
- **subscription_plan_description:** Description of the plan.

GetFirstSubscriptionPlan()

The function returns the first subscription plan name (as a string) configured on the service controller for which billing is enabled.

Example

```
var plan;
for (plan = GetFirstSubscriptionPlan(); plan != ""; plan = GetNextSubscriptionPlan(plan)) {
LoadSubscriptionPlanInformation(plan);
}
```

GetNextSubscriptionPlan(*plan_name*)

Returns the next subscription plan name that follows the specified ***plan_name***. If ***plan_name*** is the last plan, an empty string is returned.

Example

```
var plan;
for (plan = GetFirstSubscriptionPlan(); plan != ""; plan = GetNextSubscriptionPlan(plan)) {
LoadSubscriptionPlanInformation(plan);
}
```

Other

AssignBillingRecordId()

Use this function to reserve a billing record ID. If this function returns **0**, it means that the payment system has been halted. Any subscription-related activities should not be attempted until this function returns a non-zero value. See *Suspend payment system when log is full of queued records on page 8-39*).

Example

```
var billingRecordId = AssignBillingRecordId();
if (billingRecordId == 0) {
<p>The service is temporarily unavailable.Please try again later.</p>
}
```

ConditionalDisplay(*condition, state*)

This function is used to dynamically control execution of a block of code based on the value of a logical expression. An effective use for this function is to control blocks of display code, for certain features for example, that need to be turned on/off depending on user selections.

Parameters

- **Condition:** A logical embedded Javascript expression. If the expression is true, all content between the **Begin** and **End** function calls is executed.
- **State:** Indicates if this function marks the beginning or end of the block of code.
  - **Begin:** Marks the beginning of the code block.
  - **End:** Marks the end of the code block.

Example

```
<% ConditionalDisplay(client_state == 1, "begin"); %>
<p> Welcome to the wireless network.</p>
<% ConditionalDisplay(client_state == 1, "end"); %>
```

GetUserName()

Returns the username for the current user.

GetAuthenticationErrorMessage()

Reserved for use by **fail.asp** to display error messages for certain specific conditions. Do not use this function on other pages. Instead, use **LoadFormFieldError()** or **GetSessionVar** with the variable **last_login_error.**

IncludeAsp(*filename*)

Pauses ASP processing in the current file and continue with the specified ASP **filename**.

Example

```
IncludeAsp("file.asp");
```

SetSessionRefreshInterval(sec)

Specifies the refresh interval for the session page in seconds.

write(*string*)

Writes the specified string to the browser.

Example

```
write("<p>You are connected.</p>");
```

LoadAccessInformation()

This function initializes a set of variables that provide information on the site access options configured on the **Service Controller >> Public access > Web content** page.

ASP variables

- **access_free:** Set to 1 if the **Free Access** option is enabled.
- **access_purchase:** Set to 1 if the **Allow creation of user accounts** option is enabled.

Example

```
LoadAccessInformation();
if (access_free) {
<p>Welcome to your free trial of the new high-speed wireless network service.</p>
}
```

LoadPaymentInformation()

This function initializes a set of variables that provide information on the current payment services configured on the **Service Controller >> Public access > Payment services** page.

ASP variables

- **payment_currency:** Contains the 3-letter code identifying the currency that will be used for all transactions.
- **payment_cc_gateway:** Returns a string that identifies the payment service that is configured. Either **authorize.net** or **worldpay**.

Example

```
LoadPaymentInformation();
if (payment_currency == "USD") {
  write(subscription_plan_fee + " $");
}
```

LoadWorldPayInformation()

This function initializes a set of variables that contain WorldPay-specific information.

ASP variables

- **worldpay_url:** String containing the configured WorldPay URL on the service controller.
- **worldpay_installation_id:** String containing the configured WorldPay Installation ID on the service controller.
- **worldpay_cart_id:** String containing a unique number for this order that represents a virtual cart in which items that are being bought are stored.

Example

```
LoadWorldPayInformation();
write(worldpay_url);
```

LoadTaxInformation()

This function initializes a variable that provide information on the current tax setting configured on the **Service Controller >> Public access > Payment services** page.

ASP variable

- **tax_percent:** Tax rate that will be applied to all charges. The tax rate is configured on the service controller.

Example

```
LoadTaxInformation();
write("Tax is " + tax_percent + "% here.");
```

Session information

The service controller maintains a block of data, called a session, for each IP address that is connected to the public access interface. The session makes it possible to store and access data across more than one page in the public access interface.

Session variables are reset when:

- the ASP function ClearSessionVar() is called
- the user's session is deleted or restarted

A session ends when 3 minutes passes without any user activity on the public access interface.

Session functions

GetSessionVar(*variable*)

Returns the value of the specified session variable.

ClearSessionVar(*variable*)

Clears the value of the specified session variable.

Session variables

The following session variables are provided:

- **last_login_error:** Contains the error number generated by the last login attempt. This is converted into the appropriate visual representation by the file **login_error_messages.asp**.

Value	Description
0 or ""	No error occurred.
1	A problem occurred that caused the current login process to stop before it completed. This is normally an issue related to an administrator changing the configuration which may cause a temporary failure.
2	The login was refused by the product or external authentication server.
3	The external authentication server was unreachable.

4	There is already another login from the user in progress, so this one has been stopped.
5	The user account username/password appear to be valid, however the account is invalid due to subscription plan usage being exceeded or validity limit being exceeded.
6	The user account username/password appear to be valid, however the associated account is administratively disabled.

- **username:** Contains the username a user submitted to login or define a subscription.
- **password:** Contains the password, as a sting of asterisks (***), a user submitted to login or define a subscription.
- **card_expiration:** Contains credit card expiration information in the form **mm/yy**.
- **card_number:** Contains the credit card number. The string contains all asterisks (*) with only the last four digits not hidden.
- **payment_method:** Contains the user's choice for payment method: Currently only supports the value: "CreditCard".
- **subscription_plan:** This variable hold the name of the subscription plan submitted in a subscription form.
- **cart_id:** Holds the cart ID for WorldPay payments. The cart ID is automatically generated and needs to be transmitted to the WorldPay Web site via a form. See the code in **payment.asp** for an example of how to do this.
- **authorize_net_reason:** Contains a text message indicating why the Authorize.Net credit card gateway refused a payment transaction.
- **authorize_net_transaction_id:** Contains the transaction ID that the Authorize.Net credit card gateway assigned to the transaction attempt. You can display this information to the user so that they can supply this information when calling for support.

- **last_subscription_error:** Contains the error number generated by the last subscription attempt. This is converted into the appropriate visual representation by the file **subscription_error_messages.asp**.

Value	Description
0 or ""	No error occurred.
1	A problem occurred that caused the current login process to stop before it completed. This is normally an issue related to an administrator changing the configuration which may cause a temporary failure.
2	The password and confirm password fields do not match.
3	The wrong password was supplied for the specified username.
4	An error occurred when creating the user account.
5	The subscription plan name is invalid.
6	The credit card payment failed.
7	The credit card payment succeeded, however an error occurred when activating the user account.
8	Reserved.
9	Reserved.
10	Same as #3, but indicates that user account creation is currently not allowed.

- **last_form_error:** Contains specific errors for each field in a form. To extract this information use the ASP functions described in under *Form errors on page 9-74*.

10

Network configuration

Contents

Port configuration 10-3
LAN port configuration 10-4
Internet port configuration 10-5

Address allocation 10-6
DHCP server (global) 10-6
DHCP relay agent 10-9

VLAN support 10-11
Types of VLANs 10-11
VLAN configuration 10-12

GRE tunnels 10-14

Bandwidth control 10-15
Internet port data rate limits 10-16
Bandwidth levels 10-16
Example 10-17

CDP 10-18

DNS 10-19
DNS servers 10-19
DNS advanced settings 10-20

IP routes 10-21
Configuration 10-21

Network address translation (NAT) 10-23
NAT security and static mappings 10-24
VPN One-to-one NAT 10-26

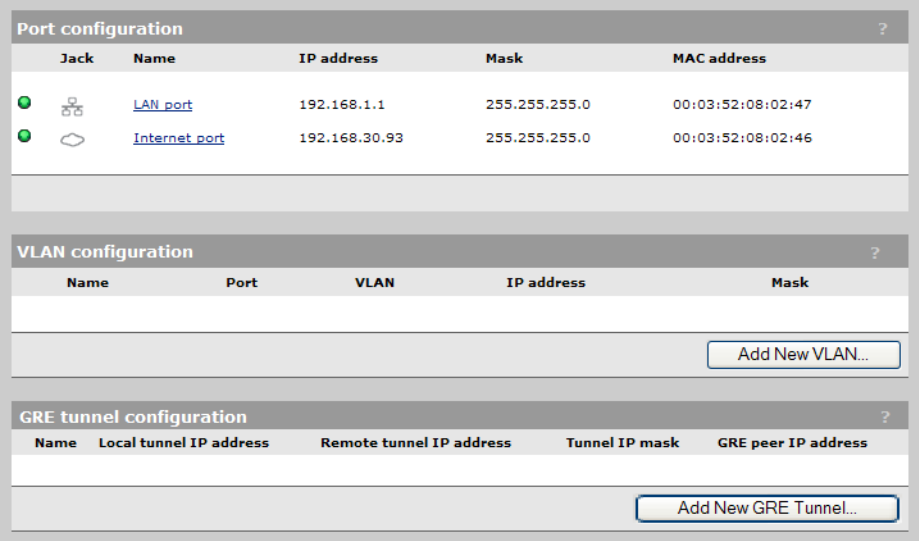
RIP 10-27

IP QoS 10-27
Configuration 10-28
Example 10-29

IGMP proxy 10-31

Port configuration

The **Port configuration** page displays summary information about all ports, VLANs, and GRE tunnels. Open this page by selecting **Service Controller >> Network > Ports**.



Port configuration information

- **Status indicator:** Operational state of each port, as follows:
  - **Green:** Port is properly configured and ready to send and receive data.
  - **Red:** Port is not properly configured or is disabled.
- **Name**: Identifier for the port. To configure a port, click its name.
- **IP address**: IP addresses assigned to the port. An address of **0.0.0.0** means that no address is assigned.
- **Mask**: Subnet mask for the IP address.
- **MAC address**: MAC address of the port.

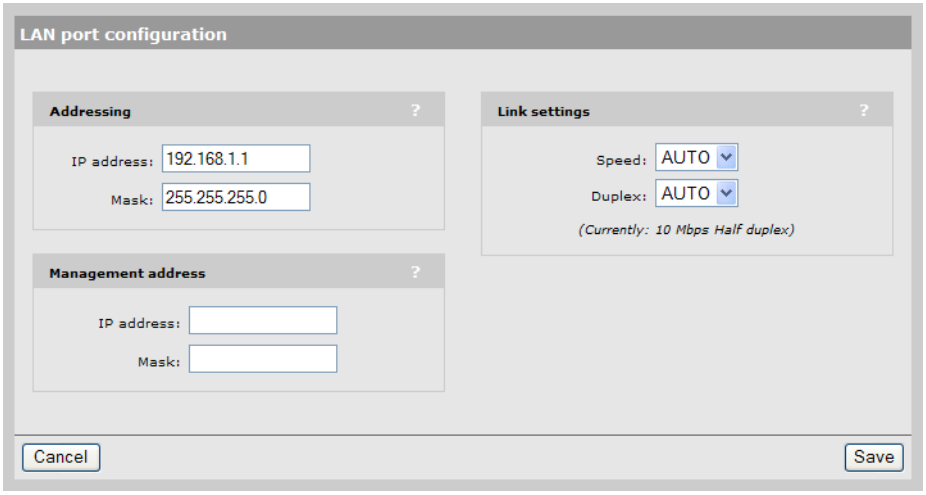
Default port settings

By default, ports are configured as follows:

Port	Default IP address	Default DHCP server status
LAN	192.168.1.1	Disabled.
Internet	DHCP client	This feature is not available on the Internet port.

LAN port configuration

The LAN port is used to connect the service controller to a wired network. To verify and possibly adjust LAN port configuration, select **Service Controller >> Network > Ports > LAN port**.



Addressing options

The LAN port must be configured with a static IP address, because the service controller cannot function as a DHCP client on the LAN port. By default it is set to the address 192.168.1.1

For information on configuring address allocation on the LAN port via DHCP server or DHCP relay agent, see *Address allocation on page 10-6*.

Management address

Use this option to assign a second IP address to the LAN port. When working with autonomous APs, this address provides a simple way to separate management traffic from user traffic without using VLANs.

For example, by default the LAN port is set to 192.168.1.1 and all client devices obtain an address on this subnet from the service controller DHCP server. With this feature you can add another address, say 192.168.2.1/255.255.255.0. Autonomous APs can then be assigned to this subnet using static IP addressing. Now all management traffic exchanged between the service controller and the APs is on a separate subnet.

Note

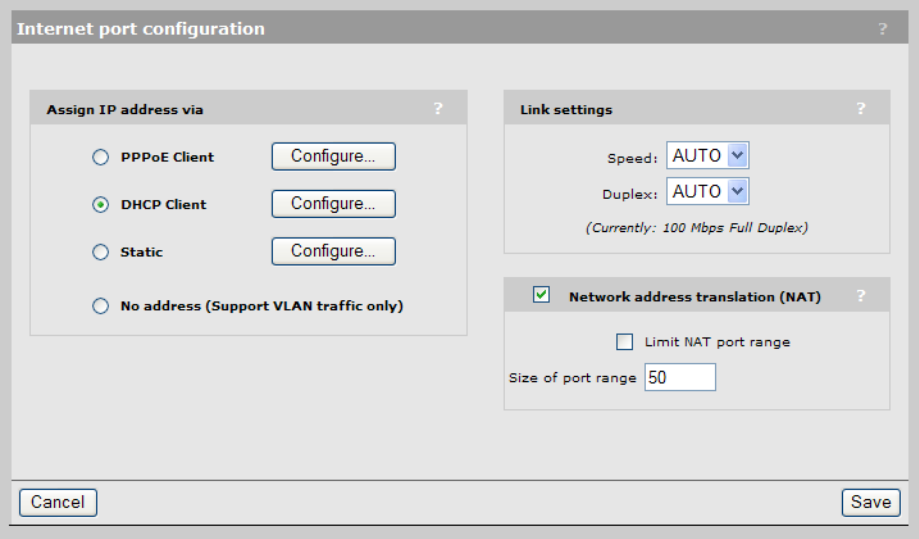
To use this address to access the management tool via the LAN port you will be required to log in via the public access interface first.

Link settings

By default, the service controller automatically adjusts link settings based on the type of equipment the port is connected to. If needed, you can force the port to operate at a particular speed or duplex setting.

Internet port configuration

To verify and possibly adjust Internet port configuration, select **Service Controller >> Network > Ports > Internet port**.



Addressing options

The Internet port supports the following addressing options:

- PPPoE client
- DHCP client (default setting)
- Static addressing
- No address.

By default, the Internet port operates as a DHCP client. Select the addressing option that is required by your ISP or network administrator and then select **Configure**. See the online help for descriptions of all configuration options.

Link settings

By default, the service controller automatically adjusts link settings based on the type of equipment the port is connected to. If needed, you can force the port to operate at a particular speed or duplex setting.

Network address translation

Enable this option to permit all the computers on the network to simultaneously share the connection on the Internet port. See *Network address translation (NAT) on page 10-23*.

Limit NAT port range

When enabled, the service controller reserves a range of TCP and UDP ports for each authenticated, access-controlled user starting at port 5000, and maps all outgoing traffic for the user within the range.

Note

- Enabling this feature only affects outgoing TCP/UDP traffic. Applications that set an incoming port (Active FTP, for example) may select a port that is outside of the allocated port range.
- If you enable this feature you should not assign static NAT mappings in the range 5000 to 10000.

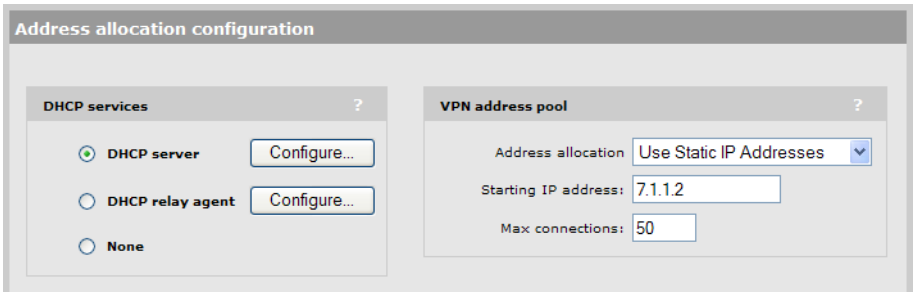
Size of port range

Sets the number of TCP and UDP ports reserved for each user.

Address allocation

The service controller can operate as a DHCP server or DHCP relay agent on the LAN port. This enables it to assign IP addresses to downstream devices connected to the LAN port.

By default, address allocation is disabled. To configure address allocation settings, select **Service Controller >> Network > Address allocation**.



For information on VPN address pool, see *Configure an IPSec profile for wireless client VPN on page 12-4*.

DHCP server (global)

The global DHCP server can be used to automatically assign IP addresses to devices that are connected to the service controller via the LAN port.

Note

Do not enable the DHCP server if the LAN port is connected to a network that already has an operational DHCP server.

A separate DHCP server can also be enabled on each VSC to assign addresses to users. See *DHCP server on page 2-20*.

The host name in the currently installed SSL certificate is automatically assigned as the domain name of the service controller. The factory default SSL certificate that is installed on the service controller has the host name **wireless.colubris.com**.

You do not have to add this name to your DNS server for it to be resolved. The service controller intercepts all DNS requests it receives. It resolves any request that matches the certificate host name by returning the IP address assigned to the Internet port. All other DNS requests are forwarded to the appropriate DNS servers as configured on the **Service Controller > Network > DNS** page.

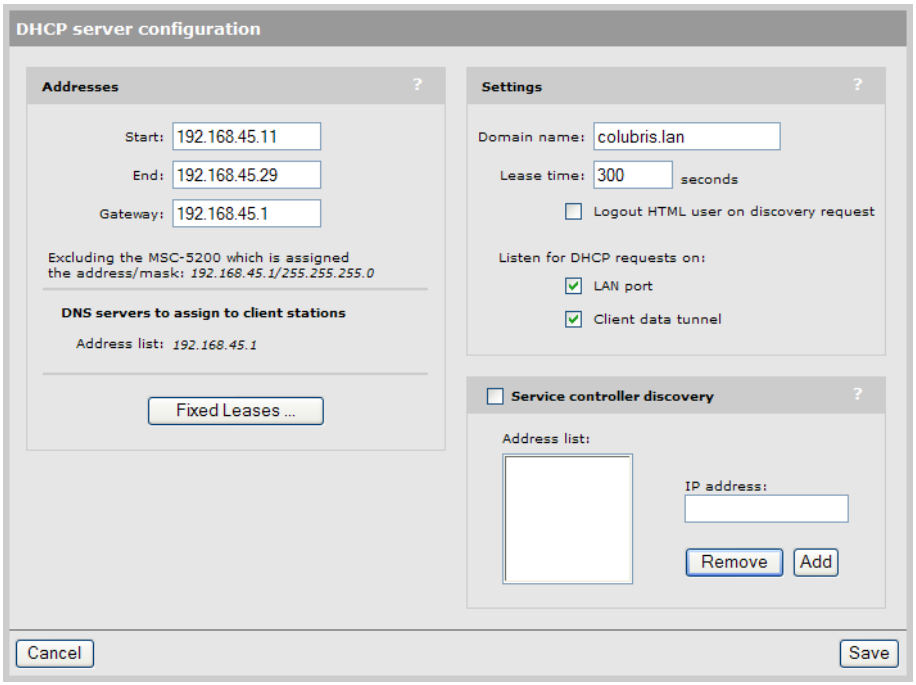
To summarize, this means that by default, any DNS request by a user that matches **wireless.colubris.com** will return the IP address of the service controller Internet port.

Note If a client station requests a new address while an active DHCP lease is already assigned to the client station, the DHCP server will not assign a new IP address, but rather will re-assign the address in the active lease.

DHCP server configuration

Configure the DHCP server as follows:

1. Select **Service Controller >> Network > Address allocation.**
2. Select **DHCP server** and then **Configure**.



3. Set the IP address of the default **Gateway** for the service controller to assign to DHCP users. You can usually specify the IP address of the service controller LAN port as the **Gateway**.

Note **DNS servers to assign to client stations** shows the IP addresses of the DNS servers that the service controller can assign to users. You can define DNS options by selecting **Network > DNS.**

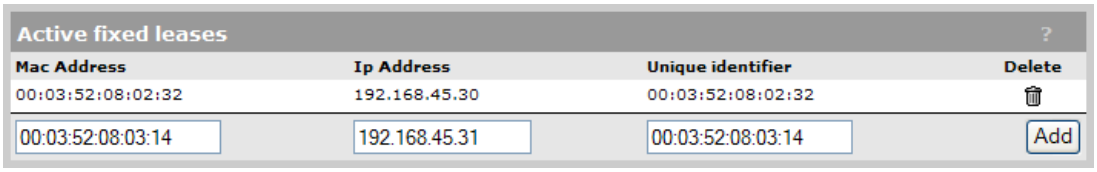
4. Adjust **Domain name** if desired. Specify the domain name for the service controller to return to users. Typically, this will be your corporate domain name.
5. Adjust **Lease time** if desired. Specify the number of seconds of lease time for the service controller to assign to all assigned addresses. Default is 300 seconds.
6. Consider enabling **Logout HTML user on discovery request** when multiple users on your network share the same device. This causes the service controller to log out a device if a DHCP discovery request is received from the device while a DHCP address lease is currently assigned. Otherwise, If a user forgets to log out before turning off the device, the next user will have to wait until the lease expires before being able to log in.
7. For **Listen for DHCP requests**, select the interfaces on which the service controller will listen for DHCP requests.
8. Select **Save**.

Note

Even when the service controller DHCP server is active, users can still connect using static IP addresses assigned on different subnets. To configure this feature, select **Public access > Access control** and under **Client options**, select **Allow any IP address**.

Active fixed leases

Use this feature to permanently reserve an IP addresses lease for a specific device. This ensures that the device is always reachable at the same address on the network, but does not require a static address to be set directly on the device itself. This table lists all permanently assigned addresses. Up to 255 fixed leases can be defined.



To assign a specific IP address to a client station specify the following and click Add:

- **MAC address**: MAC address of the client station in the format: nn:nn:nn:nn:nn:nn.
- **IP address**: IP address that will be assigned to the client station in the format: nnn.nnn.nnn.nnn.
- **Unique identifier**: An number that identifies the device. Must be unique to all DHCP clients on the network. Generally set to the MAC address of the client station. This parameter is optional unless MAC masquerading is being performed by the client station.

DHCP relay agent

The service controller provides a flexible DHCP relay implementation. It can listen for requests on the LAN port and forward them to:

- the Internet port
- an IPSec tunnel operating on the Internet port
- a GRE tunnel.

Use the following guidelines when configuring DHCP relay:

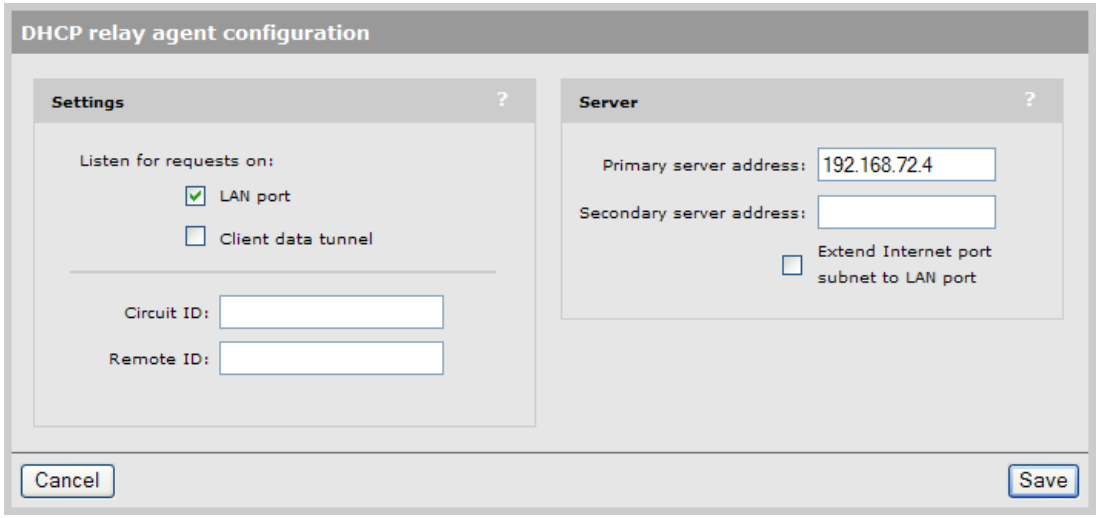
- Routes must be defined on the DHCP servers so that they can successfully send DHCP packets back to the DHCP relay agent running on the service controller. These routes must identify the segment assigned to the service controller LAN port.
- External DHCP servers must be reachable through one of the service controller ports.
- DHCP relay is not supported when PPPoE is enabled on the Internet port.
- DHCP relay cannot work if the internal firewall is set to High and NAT is enabled on the Internet port. The DHCP server must be able to ping the assigned address to prevent duplicate assignments.

A separate DHCP relay agent can also be enabled on each VSC. See *DHCP relay agent on page 2-20*.

DHCP relay agent configuration

Configure the DHCP relay agent as follows:

1. Select **Service Controller >> Network > Address allocation**.
2. Select **DHCP relay agent** and then **Configure**.



3. Under **Settings,** select the port on which the service controller listens for DHCP requests, as follows:

- **LAN port**: Listens to any requests from the local network and relays them to the remote DHCP server.
- **Client data tunnel:** Select this option when centralized access mode is enabled, and you only want to handle requests from wireless users on controlled APs. See *Client data tunnel on page 2-10*.
- **Circuit ID:** Use this field to attach information to the DHCP request that enables the server to identify the client station that issued the DHCP request. To have the service controller insert dynamic values, use the following placeholders:
  - %S: SSID the client station is associated with.
  - %B: The BSSID the client station is associated with.
  - %V: The VLAN the client station is mapped to.
- **Remote ID:** This field lets you attach information to the DHCP request which lets the server identify the service controller. To have the service controller insert dynamic values, use the following placeholders:
  - %S: SSID the client station is associated with.
  - %B: The BSSID the client station is associated with.
  - %V: The VLAN the client station is mapped to.

4. Under **Server,** configure the following parameters:
   - **Primary DHCP server address**: Specify the IP address of the first DHCP server to which the service controller should forward DHCP requests.
   - **Secondary DHCP server address**: Specify the IP address of the backup DHCP server to which the service controller should forward DHCP requests.
   - **Extend Internet subnet to LAN port**: Used to assign public IP addresses to specific clients on the LAN port. When enabled, the service controller will alter the DHCP address requests from users so that they appear to originate from the network assigned to the Internet port on the service controller. This will cause the DHCP server to assign IP addresses on this network to all users. The service controller handles all mapping between the two subnets internally.

VLAN support

Note

- This section discusses VLAN configuration on the service controller. To define VLANs on a controlled AP, see *Defining VLANs on page 3-28*.
- For information on assigning VLANs to the switch ports on an MSM317, see the *MSM137 Installation and Getting Started Guide*.

The service controller provides a robust and flexible virtual local area network (VLAN) implementation that supports a wide variety of scenarios. For example, VLANs can be used for VSC ingress and egress mappings to isolate management from user traffic. Egress VLANS can also be assigned on a per-user basis by setting the appropriate RADIUS attributes in a user's account. Up to 80 VLAN definitions can be created on the service controller. VLAN ranges are supported enabling a single definition to span a range of VLAN IDs.

The following service controller features can be supported on a VLAN:

- Network address translation (*However, static NAT mappings are not supported.)*
- Management tool access
- SNMP access
- SOAP access
- VPN traffic.

Types of VLANs

The service controller supports three types of VLANs: VSC-based VLANs, general VLANs, and user-assigned VLANs.

VSC-based VLANs

VSC-based VLANs are assigned to a VSC profile, either to an ingress or egress mapping.

- To be used as a VSC ingress, a VLAN **must not have** an IP address assigned to it.
- To be used as a VSC egress, a VLAN **must have** an IP address assigned to it.

Note

VLANs assigned in a VSC definition apply to the service controller only. On controlled APs, egress VLAN assignment for a VSC is done when the VSC is bound to the AP. See *Defining VLANs on page 3-28*.

General VLANs

General VLANs are VLANs that are not assigned to a VSC profile, which means that:

- Access control does not apply to traffic on these VLANs.
- An address must be assigned to the VLAN either via DHCP or static assignment.
- VLAN traffic is routed.

User-assigned (dynamic) VLANs

VLANs can be assigned on a per-user basis by defining the appropriate RADIUS attributes in a user's account or by setting a VLAN ID in the local user accounts (see *Defining account profiles on page 7-11*).

- Only supported for 802.1X users.
- The VLAN applies only on the controlled AP and not on the service controller.

Note

User-assigned VLANs override VLANs assigned by a VSC on the controlled AP.

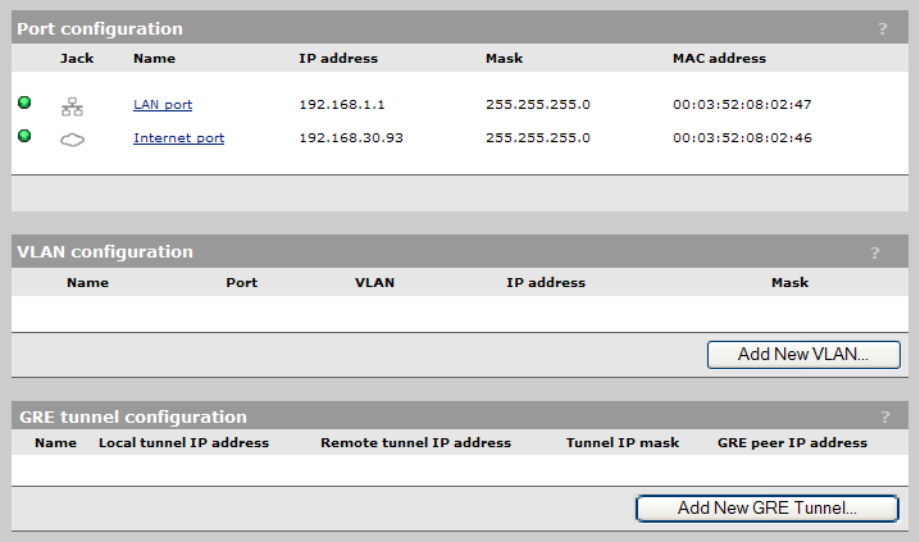
For example, if a user is assigned a VLAN of 20 via RADIUS attribute, and the AP is bound to a VSC with VLAN 30, user traffic ends up on VLAN 20. On the service controller, VLAN 20 is mapped to a VSC with egress 40, which means that the user traffic ends up on VLAN 40.

VLAN ranges

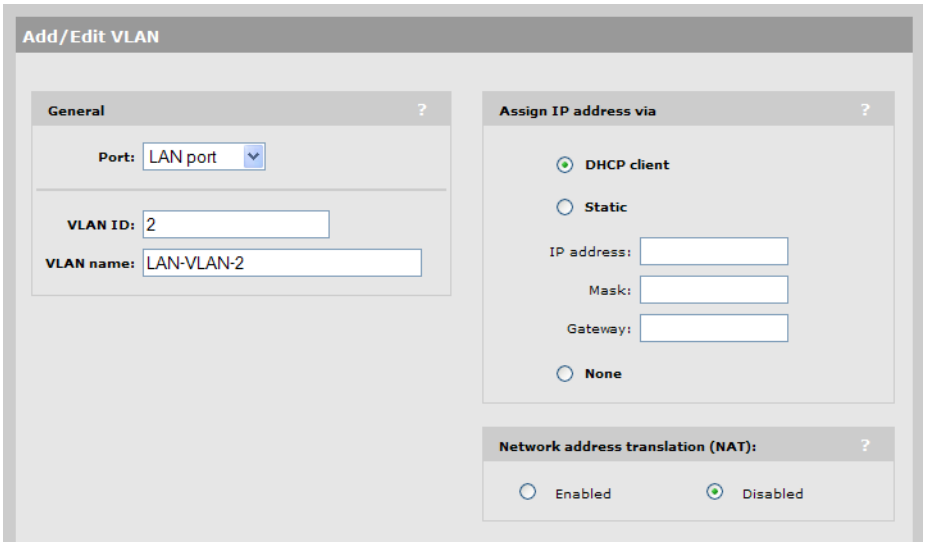
A VLAN assigned to the LAN port can be defined to cover a range of IDs (1 to 4094). This enables a single VLAN definition to accept traffic for one or more VLAN IDs, making it easy to manage a large number of contiguously assigned VLANs. You can use a VLAN range to aggregate traffic from several VLANs and assign it to the same VSC ingress. An IP address cannot be assigned to a VLAN range.

VLAN configuration

To view and configure VLAN definitions, select **Service Controller >> Network > Ports**. Initially, no VLANs are defined.



To add a VLAN, select **Add New VLAN.** The **Add/Edit VLAN** page opens.



Define VLAN settings as described in the following sections.

General

- **Port**: Select the physical interface with which the VLAN is associated. You can define a VLAN on the **Internet port** or **LAN port.**
- **VLAN ID**: Specify an 802.1Q identifier for the VLAN.

  If the VLAN is assigned to the LAN port, you can also define a range of VLANs in the form *X-Y*, where *X* and *Y* can be 1 to 4094; for example, *50-60*. This enables a single VLAN definition to accept traffic for one or more VLAN IDs, making it easy to manage a large number of contiguously assigned VLANs. You can define more than one VLAN range, but each range must be distinct and contiguous.

Note

VLANS with ranges cannot be used for **VSC egress mapping** and cannot be assigned an IP address.

- **VLAN name**: Specify a name to identify the VLAN definition on the service controller. This name has no operational significance.

Assign IP address via

Specify how the VLAN obtains an IP address, as follows:

- **DHCP client**: The VLAN obtains its IP address from a DHCP server on the same VLAN.

Note

There is no support for obtaining a default gateway from the DHCP server.

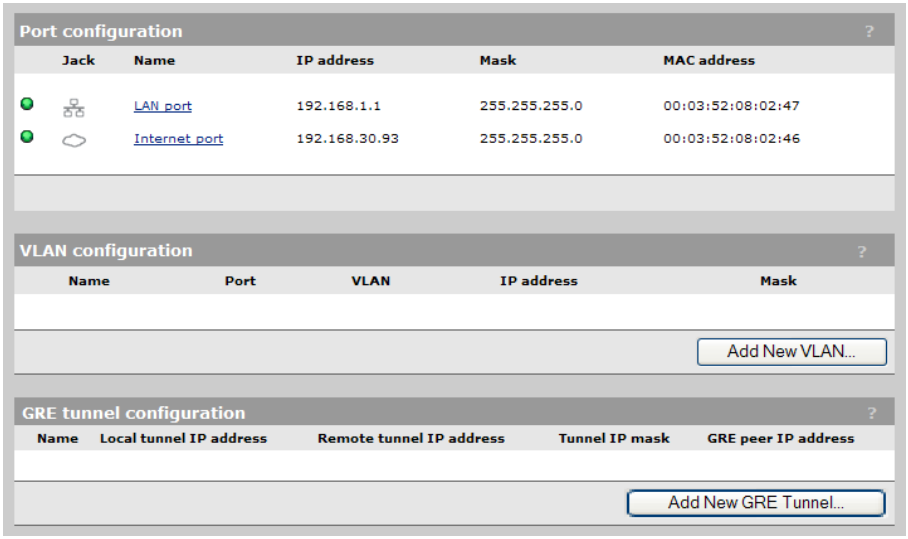
- **Static**: Enables you to manually assign an IP address to the VLAN. If you select this option, you must specify a static **IP address, Mask,** and **Gateway.**
- **None**: Specifies that this VLAN has no IP address, so that you can use the VLAN for a VSC ingress mapping.

NAT

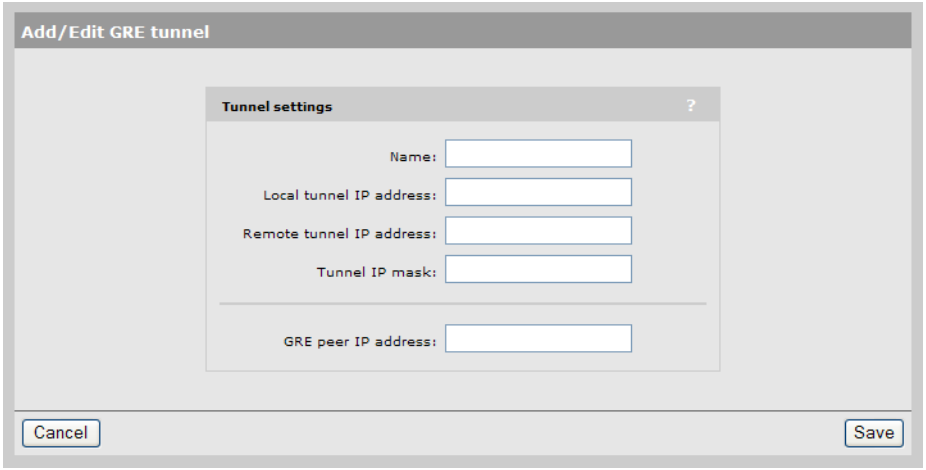
Available only if addressing is **DHCP client** or **Static.** Specify whether network address translation (NAT) is enabled on the VLAN. By default NAT is disabled**.** See *Network address translation (NAT) on page 10-23*.

GRE tunnels

To view and configure GRE tunnel definitions, select **Service Controller >> Network > Ports**. Initially, no GRE tunnels are defined.



To add a tunnel**,** select **Add New GRE Tunnel.** The **Add/Edit GRE Tunnel** page opens.



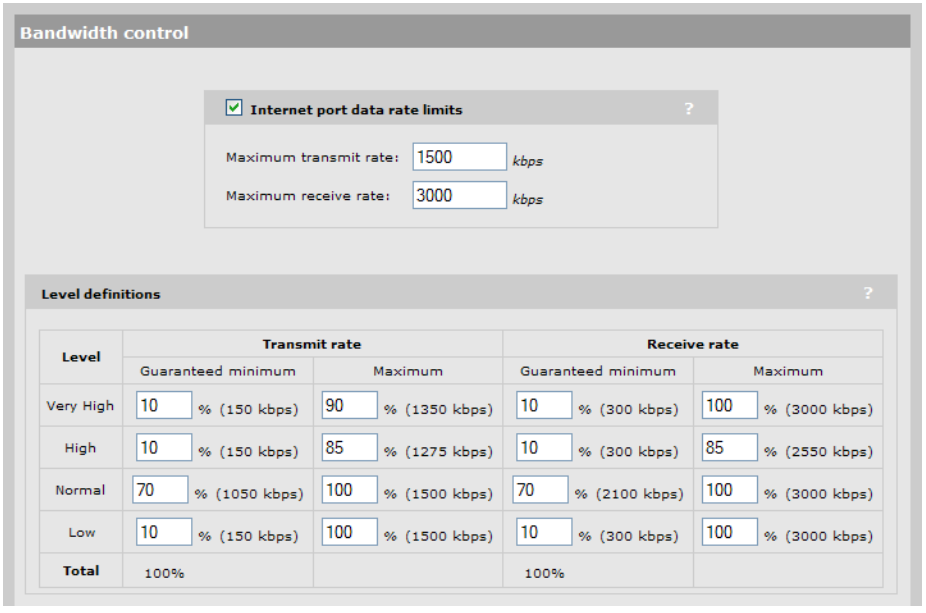
Define tunnel settings as follows:

- **Name:** Tunnel name.
- **Local tunnel IP address:** Specify the IP address of the service controller inside the tunnel.
- **Remote tunnel IP address:** Specify the IP address of the remote device inside the tunnel.
- **Tunnel IP mask:** Specify the mask associated with the IP addresses inside the tunnel.
- **GRE peer IP address:** Specify the IP address of the remote device that terminates the tunnel.

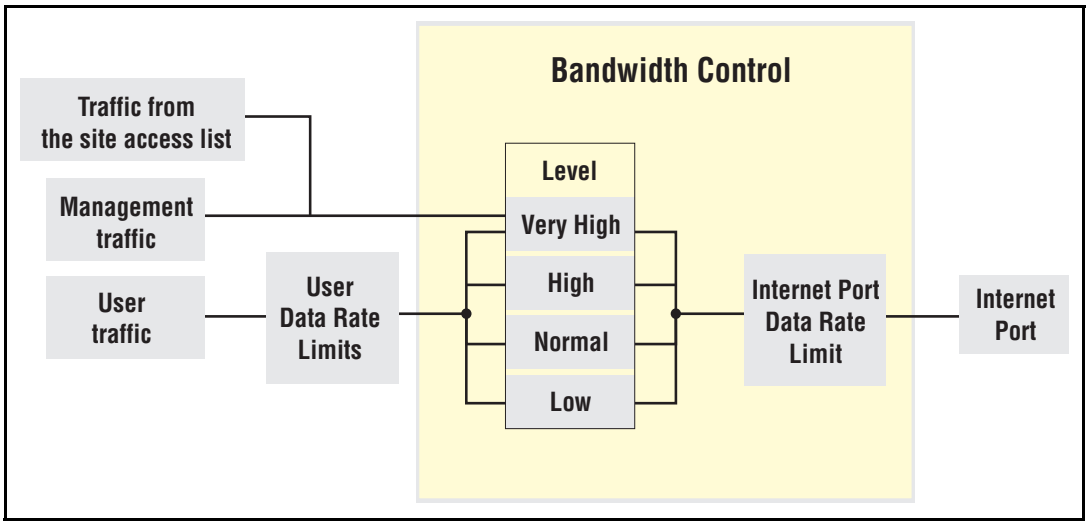
Bandwidth control

The service controller incorporates a powerful bandwidth management feature that enables comprehensive control of all user traffic flowing through the service controller.

To configure Bandwidth management, select **Service Controller >> Network > Bandwidth Control.**


Bandwidth control
Internet port data rate limits
Maximum transmit rate: 1500 kbps
Maximum receive rate: 3000 kbps
Level definitions
Level
Transmit rate
Receive rate
Guaranteed minimum
Maximum
Guaranteed minimum
Maximum
Very High 10 % (150 kbps) 90 % (1350 kbps) 10 % (300 kbps) 100 % (3000 kbps)
High 10 % (150 kbps) 85 % (1275 kbps) 10 % (300 kbps) 85 % (2550 kbps)
Normal 70 % (1050 kbps) 100 % (1500 kbps) 70 % (2100 kbps) 100 % (3000 kbps)
Low 10 % (150 kbps) 100 % (1500 kbps) 10 % (300 kbps) 100 % (3000 kbps)
Total 100% 100%

Bandwidth control has two separate components: Internet port data rate limits and bandwidth levels. They interact with the data stream as follows:



Internet port data rate limits

These settings enable you to limit the total incoming or outgoing data rate on the Internet port. If traffic exceeds the rate you set for short bursts, it is buffered. Long overages will result in data being dropped.

To utilize the full available bandwidth, the Maximum transmit rate and Maximum receive rate should be set to match the incoming and outgoing data rates supported by the connection established on the Internet port.

Bandwidth levels

The service controller provides four levels of traffic priority that you can use to manage traffic flow: *Very High*, *High*, *Normal*, and *Low*. The settings for each level are customizable, allowing performance to be tailored to meet a wide variety of scenarios.

Assigning traffic to a bandwidth level

Traffic is assigned to a bandwidth level for each VSC or for each user. Each VSC can be configured to handle user traffic at a specific bandwidth level. This level applies to users who do not have a specific assignment in their RADIUS account.

- Management traffic (which includes RADIUS, SNMP, and administrative sessions) is assigned to bandwidth level Very High and cannot be changed.
- All traffic assigned to a particular bandwidth level shares the allocated bandwidth for that level across all VSCs. This means that if you have three VSCs all assigning user traffic to High, all users share the bandwidth allocated to the High level.

Customizing bandwidth levels

Bandwidth levels are arranged in order of priority from Very High to Low. Priority determines how free bandwidth is allocated once the minimum rate is met for each level. Free bandwidth is always assigned to the higher priority levels first.

Bandwidth rates for each level are defined by taking a percentage of the maximum transmit and receive rates defined for the Internet port. Each bandwidth level has four rate settings:

- Transmit rate - guaranteed minimum: Minimum amount of bandwidth that will be assigned to a level as soon as outgoing traffic is present on the level.
- Transmit rate - maximum: Maximum amount of outgoing bandwidth that can be consumed by the level. Traffic in excess is buffered for short bursts, and dropped for sustained overages.
- Receive rate - guaranteed minimum: Minimum amount of bandwidth that will be assigned to a level as soon as incoming traffic is present on the level.
- Receive rate - maximum: Maximum amount of incoming bandwidth that can be consumed by the level. Traffic in excess is buffered for short bursts, and dropped for sustained overages.

Example

For example, assume that transmit bandwidth is configured as follows:

	Transmit rates	
	Min	**Max**
Very High	20	20
High	40	100
Normal	20	100
Low	20	20

Next, assume the following bandwidth requirement occurs on transmitted user data:

- High requires 70%, which is 30% more than its minimum.
- Normal requires 50%, which is 30% more than its minimum.
- There is no traffic on Very High or Low.

Since both High and Normal require bandwidth in excess of their guaranteed minimum, each is allocated their guaranteed minimum. This leaves 40% of the bandwidth free to be assigned on a priority basis. High has more priority than Normal, so it takes as much bandwidth as needed. In this case it is 30%, which brings High up to 70%. This leaves 10% for Normal, which is not enough. Traffic is buffered for a short period, and then dropped.

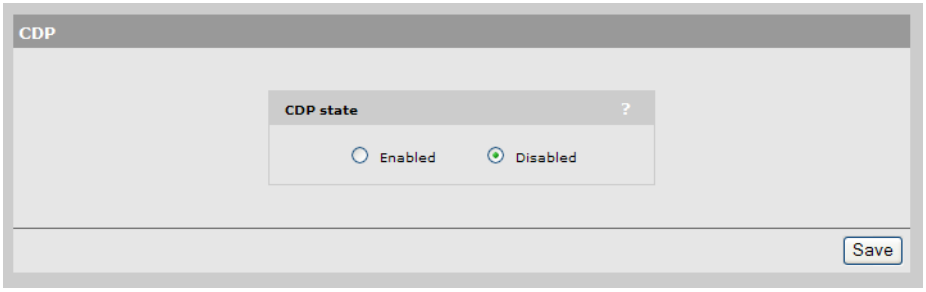
If at the same time Very High traffic is sent, this level immediately steals 20% from the lower levels. In this case, 10% is taken from Normal, returning it to its minimum guaranteed level, and 10% is taken from High.

CDP

The service controller can be configured to transmit CDP (Cisco Discovery Protocol) information on the LAN and Internet ports. This information is used to advertise service controller information to third-party devices, such as CDP-aware switches.

The service controller uses CDP information sent by autonomous APs to collect information about these APs for display on the **Management > Satellites** page.

To enable CDP transmission, select **Service Controller >> Network > CDP.**

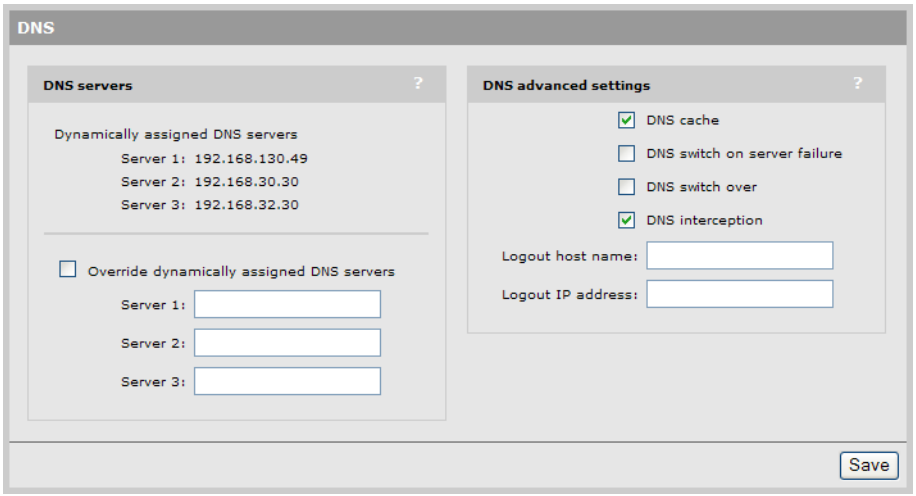


Note

- The service controller always listens for CDP information on the LAN and Internet ports, even when this option is disabled, to build a list of autonomous APs. CDP information from third-party devices and controlled APs is ignored.
- Controlled APs always send CDP information.

DNS

The service controller provides several options to customize DNS handling. To configure these options, select **Service Controller >> Network > DNS.**



DNS servers

- **Dynamically assigned servers**: Gives information about the DNS servers that are assigned to the service controller. This option does not appear if static addressing is in use.
- **Override dynamically assigned DNS servers**: Enable this checkbox to use the DNS servers that you specify on this page to replace those that are assigned to the service controller. This option does not appear if static addressing is in use.
  - **Server 1**: Specify the IP address of the primary DNS server for the service controller to use.
  - **Server 2**: Specify the IP address of the secondary DNS server for the service controller to use.
  - **Server 3**: Specify the IP address of the tertiary DNS server for the service controller to use.

Note

When using Active Directory, the DNS servers should be the Active Directory servers or the devices that provide SRV records.

DNS advanced settings

- **DNS cache**: Enable this checkbox to activate the DNS cache. Once a host name is successfully resolved to an IP address by a remote DNS server, it is stored in the cache. This speeds up network performance, because the remote DNS server does not have to be queried for subsequent requests for this host.

  An entry stays in the cache until one of the following is true:

  - An error occurs when connecting to the remote host.
  - The time to live (TTL) of the DNS request expires.
  - The service controller restarts.

- **DNS switch on server failure**: Controls how the service controller switches between servers:

  - When enabled, the service controller switches servers if the current server replies with a DNS server failure message.
  - When disabled, the service controller switches servers if the current server does not reply to a DNS request.

- **DNS switch over**: controls how the service controller switches back to the primary server.

  - When enabled, the service controller switches back to the primary server once the primary server becomes available again.
  - When disabled, the service controller switches back to the primary server only when the secondary server becomes unavailable.

- **DNS interception**: When enabled, the service controller intercepts all DNS requests and relays them to the configured DNS servers. DNS interception must be enabled to support:

  - Redirection of users to the public access interface login page when the service controller cannot resolve the domain requested by the user. For example, if the user is using a private or local domain as the default home page in its browser.
  - Users configured to use HTTP proxy.
  - Users with static IP addresses when the **Allow any IP address** option is enabled on the **Public access > Access control** page.

  When disabled, the service controller does not intercept any DNS requests, enabling devices to use a DNS server other than the service controller. To support this option, you must set **Network > Address allocation** to **DHCP relay agent** or **Static**.

Note

When **Network > Address allocation** is set to **DHCP Server** the service controller always returns its own address as the DNS server. Disabling DNS interception in this case causes all DNS requests to fail.

IP routes

The routing module on the service controller provides the following features:

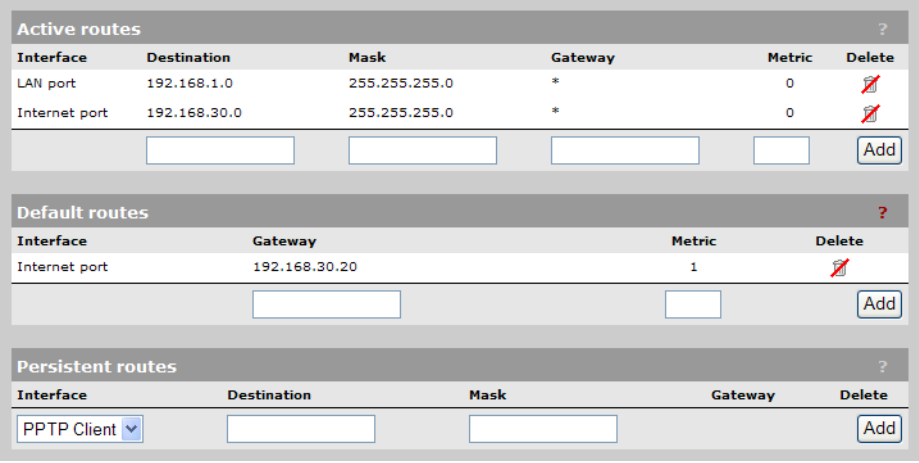
- Compliance with RFC 1812, except for multicast routing
- Supports Classless Inter Domain Routing (CIDR)
- Supports Routing Internet Protocol (RIP) versions 1 and 2 in active or passive mode.

Output from the router is sent to the appropriate logical interface based on the target address of the traffic. Supported logical interfaces include:

- VLAN
- Untagged
- IPSec client
- PPTP client
- GRE tunnel.

Configuration

To view and configure IP routes, select **Service Controller >> Network > IP routes**.



Active routes

This table shows all active routes on the service controller. You can add routes by specifying the appropriate parameters and then selecting **Add.**

The routing table is dynamic and is updated as needed. This means that during normal operation the service controller adds routes to the table as required. You cannot delete these system routes.

The following information is shown for each active route:

- **Interface**: The port through which traffic is routed. When you add a route, the service controller automatically determines the interface to be used based on the **Gateway** address.
- **Destination**: Traffic addressed to this IP address is routed.
- **Mask**: Number of bits in the destination address that are checked for a match.
- **Gateway**: IP address of the gateway to which the service controller forwards routed traffic (known as the next hop).

  An asterisk is used by system routes to indicate a directly connected network.

  Routes cannot be manually specified for IPSec. These routes are automatically added by the system based on the settings for the IPSec security association.
- **Metric**: Priority of a route. If two routes exist for a destination address, the service controller chooses the one with the lower metric.

Default routes

The **Default routes** table shows all default routes on the service controller. Default routes are used when traffic does not match any route in the Active routes table. You can add routes by specifying the appropriate parameters and then selecting **Add.**

The routing table is dynamic and is updated as needed. If more than one default route exists, the first route in the table is used.

The following information is shown for each default route:

- **Interface**: The port through which traffic is routed. When you add a route, the service controller automatically determines the interface to be used based on the **Gateway** address.
- **Gateway**: IP address of the gateway to which the service controller forwards routed traffic (known as the next hop).

  An asterisk is used by system routes to indicate a directly connected network.
- **Metric**: Priority of a route. If two routes exist for a destination address, the service controller chooses the one with the lower metric.

Persistent routes

Persistent routes are automatically deleted and then restored each time the interface they are associated with is closed and opened. When the routes are active, they also appear in the Active routes table.

PPTP client

The service controller provides an **Auto-route discovery** option to enable it to automatically discover and add routes for IP addresses on the other side of a Point-to-Point Tunnelling Protocol (PPTP) tunnel. The addresses must be part of the remote domain as specified on the **Service Controller >> VPN > PPTP client** page. Routes are added only when an attempt is made to access the target addresses.

About PPTP client routes (Internet port)

If you disabled the **Auto-route discovery** option (**VPN > PPTP client**), or if you need to access IP addresses that are not part of the specified domain, you must define the appropriate persistent routes.

About PPTP server routes (Internet port)

Activation of the route can be triggered by a specific username. When a user establishes a connection with the service controller PPTP server, its username is checked against the persistent routes list and if a match is found, the route is enabled.

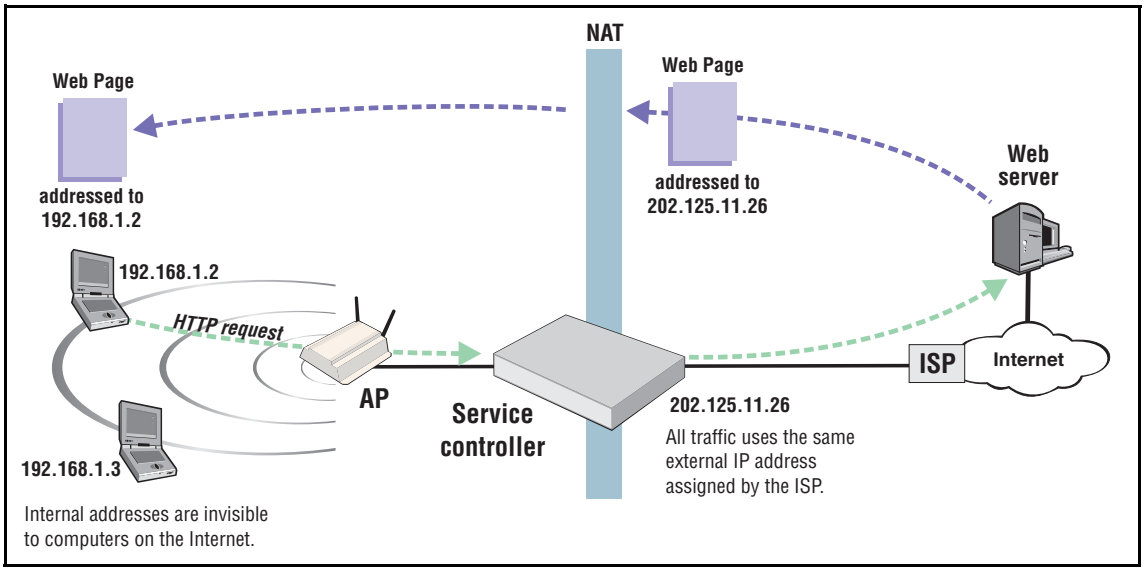
Network address translation (NAT)

Network address translation is an address mapping service that enables one set of IP addresses to be used on an internal network, and a second set to be used on an external network. NAT handles the mapping between the two sets of addresses.

Generally NAT is used to map all addresses on an internal network to a single address for use on an external network like the Internet. The main benefits are that NAT:

- Enables several devices to share a single connection
- Effectively hides from the outside network the IP addresses of all devices on the internal network.

This is illustrated as follows:



NAT can be useful in conjunction with virtual private network (VPN) connections. When two networks are connected through a VPN tunnel, it may be desirable to obscure the address of local computers for security reasons.

NAT security and static mappings

One of the benefits of NAT is that it effectively hides the IP addresses of all computers on the internal network from the outside network. In some cases, however, it is useful to make a computer on the internal network accessible externally. For example, a Web server or FTP server.

Static NAT mapping addresses this problem. Static NAT mapping enables you to route specific incoming traffic to an IP address on the internal network. For example, to support a Web server, you can define a static NAT mapping to route traffic on TCP port 80 to an internal computer running a Web server.

A static NAT mapping allows only one internal IP address to act as the destination for a particular protocol (unless you map the protocol to a nonstandard port). For example, you can run only one Web server on the internal network.

Note

- If you use a NAT static mapping to enable a secure (HTTPS) Web server on the internal network on TCP port 443, remote access to the **management tool** is no longer possible, as all incoming HTTPS requests are routed to the internal Web server and not to the **management tool. You can change the default management port (TCP 443) to an alternate unused TCP port in this case.**
- If you create a static mapping, the firewall is automatically opened to accept the traffic. However, this firewall rule is not visible on the Firewall configuration page.

Common applications are affected by NAT as follows:

Application	NAT
FTP (passive mode)	Requires a static mapping to function.
FTP (active mode)	Requires a static mapping to function.
NetMeeting	Requires a static mapping to function.
Telnet	Requires a static mapping to function.
Windows networking	No effect

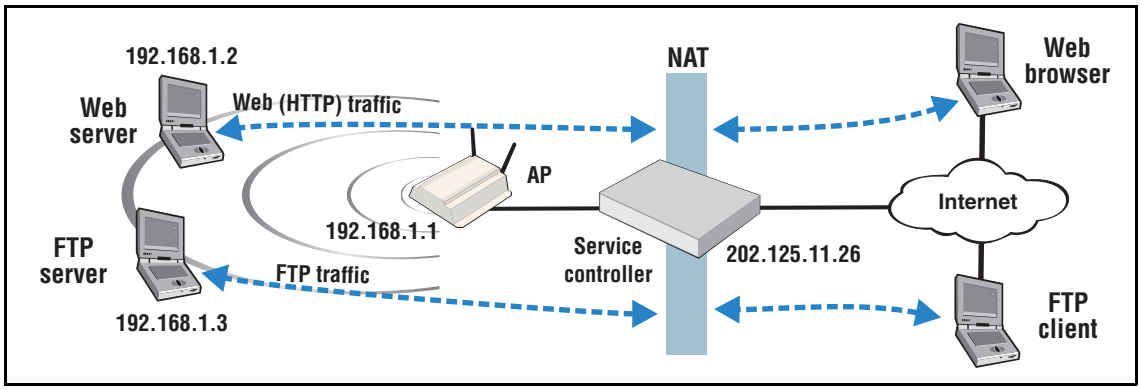
The service controller provides pre-configured static mappings for most common applications, which you can enable as needed.

Most Web browsers use FTP in active mode. Some browsers provide a configuration option that enables you to alter this. Use the following steps to change this behavior in Microsoft Internet Explorer.

1. Select **Tools > Internet options** to open the **Internet options** dialog.
2. Select the **Advanced** tab.
3. Under **Browsing,** enable the **Use Passive FTP for compatibility with some firewalls and DSL modems** checkbox.

NAT example

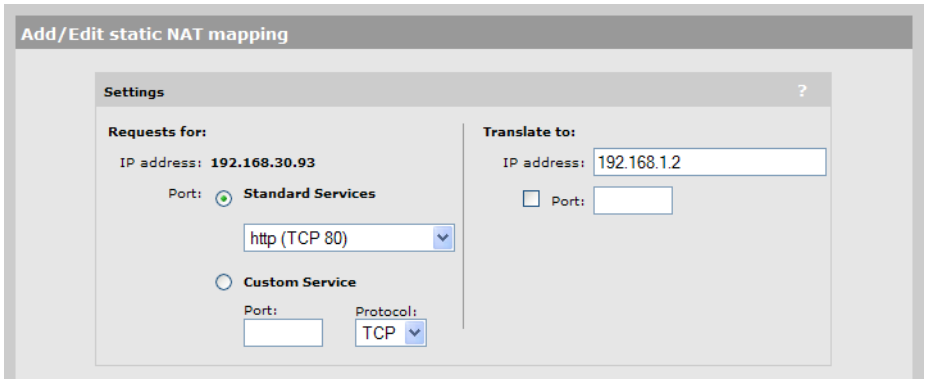
The following example shows you how to configure static NAT mappings to run a Web server and an FTP server on the internal network. This scenario might occur if you use the service controller in an enterprise environment.



By creating static NAT mappings, FTP and HTTP (Web) traffic can be routed to the proper user. Note that the addresses of these stations are still not visible externally. Remote computers send their requests to 202.125.11.26, and the service controller routes them to the proper client.

Use the following steps to configure the service controller to support this example,.

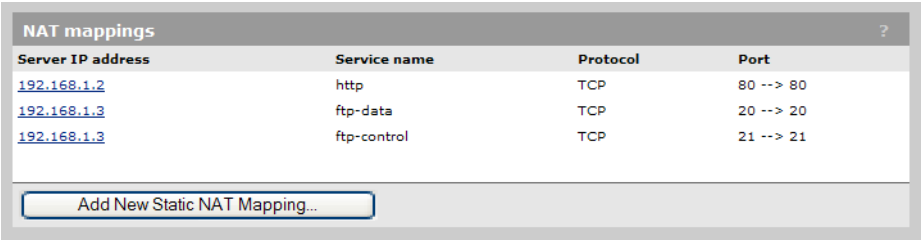
1. Select **Service Controller >> Network > NAT** > **Add New Static NAT Mapping**.
2. On the NAT mappings page, select **Add New Static NAT Mapping**.
3. Under **Requests for**, select **Standard Services**, and then select **http (TCP 80).**
4. Under **Translate to**, specify the IP address of the Web server, for example **192.168.1.2.** The Settings box should now look similar to this:



5. Select **Add** to save your changes and return to the NAT mappings page. The new mapping is added to the table.

6. To support the FTP server, create two additional mappings with the following values:
   - Set **Standard Services** to **ftp-data (TCP 20)** and set **IP address** to **192.168.1.3**.
   - Set **Standard Services** to **ftp-control (TCP 21)** and set **IP address** to **192.168.1.3**.

   The NAT mappings table should now show all three mappings:



VPN One-to-one NAT

This feature can only be used with authenticated, access-controlled users. It is only supported when a static IP address is assigned to the Internet port. (It is configured by selecting **Network > Ports > Internet port > Static > Additional IP addresses**.)

When this feature is enabled, the service controller can assign a unique IP address to each IPSec or PPTP VPN connection made by a user to a remote server via the Internet port. Addresses are assigned as defined in the **Address pool**.

To reduce the number of addresses that need to be defined, the service controller will use the same address for multiple users as long as they are establishing a connection with different VPN servers.

Use this feature when all of the following conditions are true:

- Users intend to make IPSec or PPTP VPN connections with a remote site via the service controller Internet port.
- NAT is enabled on the service controller.

  In its default configuration, NAT translates all IP address on the local network to a single public IP address: the address assigned to the service controller Internet port. As a result, all user sessions to an external resource appear to originate from the same IP address. This can cause a problem with remote VPN servers that require a unique IP address for each user session.
- The remote VPN server requires that each user have a unique IP address.

Assigning addresses to client stations

To make use of this feature, each user account must have the **VPN one-to-one NAT** option enabled.

- If using the local user accounts (defined on the **Service controller >> Users** menu), enable **VPN one-to-one NAT** in the account profile that is assigned to the user.

- If using a RADIUS server, add a Colubris AV-Pair to the user's account with the value `one-to-one-nat=1`. See *Default user one-to-one NAT on page 9-50*.

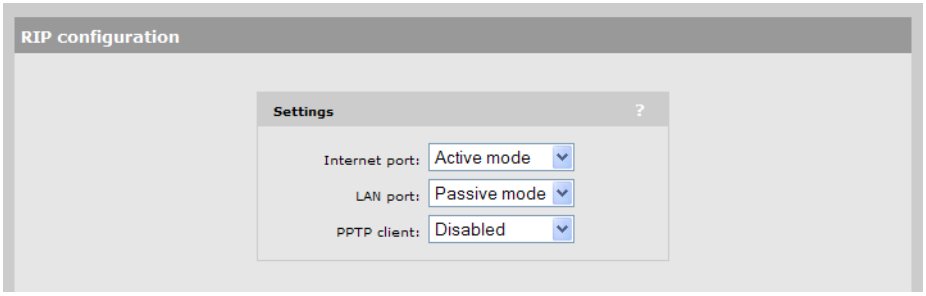
Note External devices cannot initiate connections with internal client stations via the address assigned using this feature.

RIP

The service controller supports Routing Information Protocol (RIP) versions 1 and 2. RIP can operate in one of two modes on the interfaces you select.

- **Passive mode**: The service controller listens for routing broadcasts to update the routing table, but does not broadcast its own routes.
- **Active mode**: The service controller listens for routing broadcasts to update the routing table, and also broadcast its own routes.

For example:



Note RIP is not supported if you are using PPPoE on the Internet port.

IP QoS

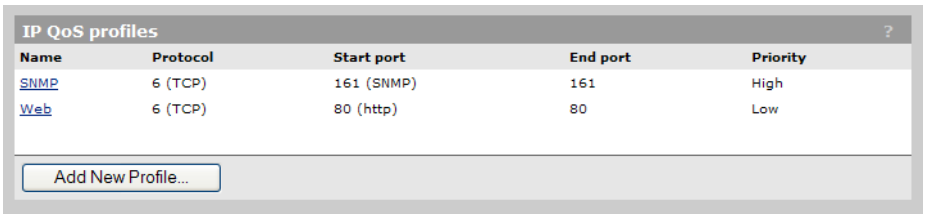
To ensure that critical applications have access to the required amount of wireless bandwidth, you can classify packets destined for the wireless interface into priority queues based on a number of criteria. For example, you can use any of the following to place data packets in one of four priority queues for transmission onto the wireless interface:

- TCP source port
- UDP source port
- Destination port
- Port ranges

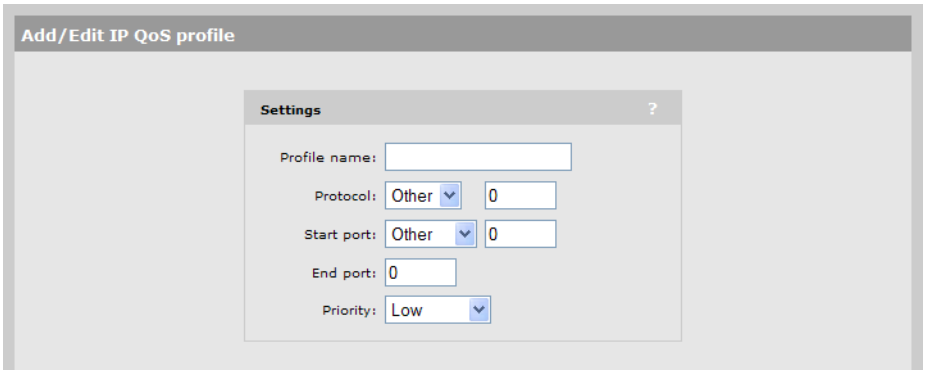
You configure IP quality of service (QoS) by creating IP QoS profiles that you can then associate with VSCs or use for global wireless settings. You can configure as many as 32 IP QoS profiles on the service controller. You can associate as many as 10 IP QoS profiles with each VSC.

Configuration

To view and configure IP QoS profiles, select **Service Controller >> Network > IP QoS**. Initially, no profiles are defined.



To create an IP QoS profile select **Add New Profile**.



Settings

- **Profile name:** Specify a unique name to identify the profile.
- **Protocol:** Specify an IP protocol to use to classify traffic by specifying its Internet Assigned Numbers Authority (IANA) protocol number. Protocol numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually. You can find IANA-assigned protocol numbers on the Internet.
- **Start port/ End port:** Optionally specify the first and last port numbers in the range of ports to which this IP QoS profile applies. To specify a single port, specify the same port number for both **Start port** and **End port.** Port numbers are pre-defined for a number of common protocols. If the protocol you require does not appear in the list, select **Other** and specify the appropriate number manually.

Note

To accept traffic on all ports for a specified protocol, set **Start port** to **Other** and **0.** Also set **End port** to 65535.

- **Priority:** Select the priority level that will be assigned to traffic that meets the criteria specified in this IP QoS profile.

Note

It is strongly recommended that you reserve **Very high** priority for voice applications.

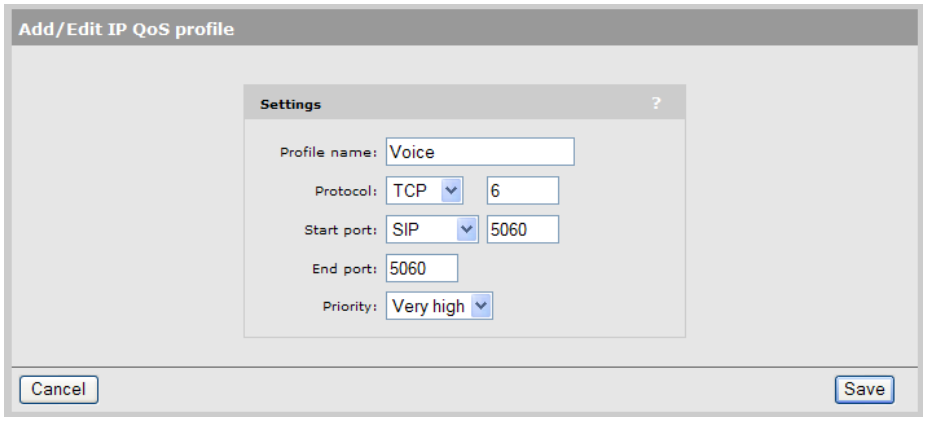
Example

This example shows how to create two IP QoS profiles and associated them with a VSC. The two profiles are:

- **Voice**: Provides voice traffic with high priority.
- **Web:** Provides HTTP traffic with low priority.

Create the profiles

1. Select **Network > IP QoS,** and then **Add New Profile.** The **IP QoS Profile** page opens.
2. Under **Profile name,** specify **Voice.**
3. Under **Protocol,** from the drop-down list select **TCP.**
4. Under **Start port,** from the drop-down list select **SIP. Start port** and **End port** are automatically populated with the correct value: **5060.**
5. Under **Priority,** from the drop-down list select **Very High.**



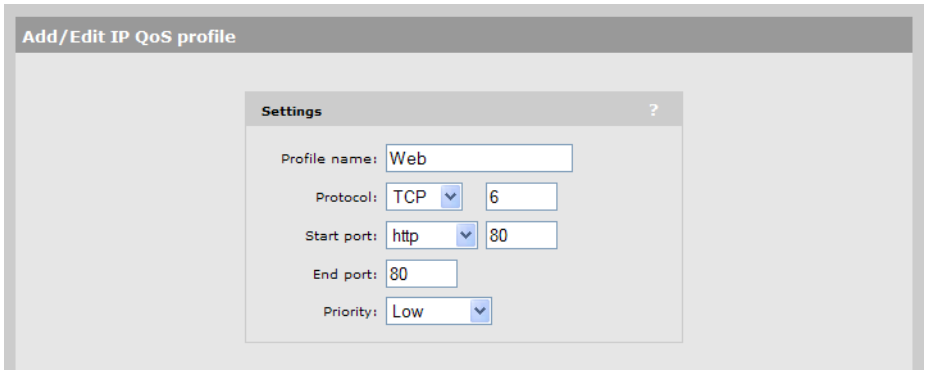
6. Select **Save.**

Note

You could also create another profile using the same parameters but for UDP to cope with any kind of SIP traffic.

7. On the **IP QoS Profile** page select **Add New Profile.**
8. Under **Profile name,** specify **Web.**
9. Under **Protocol,** from the drop-down list select **TCP.**
10. Under **Start port,** from the drop-down list select **http. Start port** and **End port** are automatically populated with the common HTTP port, **80.**

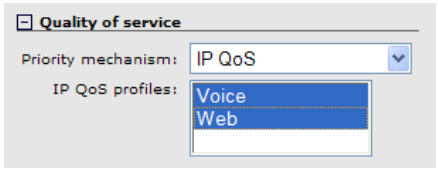
11. Under **Priority,** from the drop-down list select **Low.**



12. Select **Save.**

Assign the profiles to a VSC

1. In the **Network Tree** select **VSCs** (if not visible, first click the + symbol to the left of **Service Controller**), and then select one of the VSC profiles in the **Name** column. Scroll down to the **Quality of service** section of the **Virtual AP** box.



2. Set **Priority mechanism** to **IP QoS.**
3. in **IP QoS profiles**, Ctrl-click each profile .
4. Select **Save.**

IGMP proxy

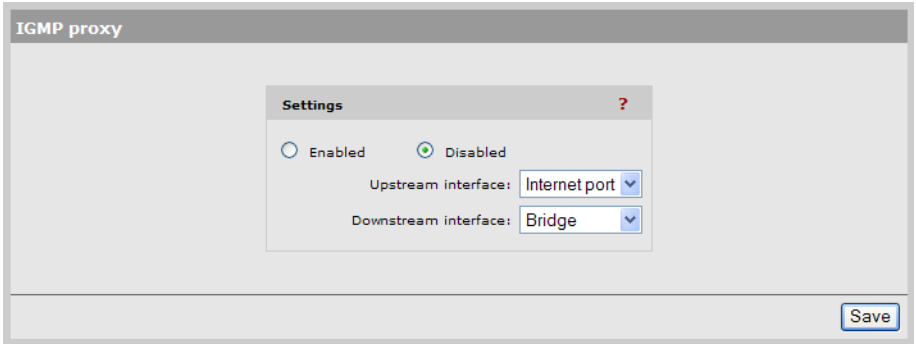
This feature provides support for multicast routing using IGMP (Internet Group Management Protocol), which is typically required by the service controller. When enabled, IGMP:

- Routes all multicast traffic received on the Upstream interface to the Downstream interface.
- Listens for IGMP host membership reports from authenticated users on the Downstream interface and forwards them to the Upstream interface. IGMP host membership reports from unauthenticated users are ignored.

Note

- An access list definition must be created to accept the multicast traffic (video streams, etc.)
- Due to the nature of multicast traffic, once a user registers for a stream it automatically becomes visible to unauthenticated users as well. However, unauthenticated users are not able to register with the IGMP group.

To view and configure IGMP proxy settings, select **Service Controller >> Network > IGMP proxy**.



11

Wireless mobility

Contents

Mobility license 11-2

Key concepts 11-2

WPA2 Opportunistic key caching 11-2

Layer 3 Mobility 11-3

Wireless mobility scenario 11-3

Mobility license

If you purchased an MSM7xx Mobility Controller, the Mobility license is factory-installed. You do not need to install a license. For MSM7xx Access Controllers, you can purchase an optional Mobility license. An MSM7xx Access Controller with an installed Mobility license, is functionally identical to the corresponding MSM7xx Mobility Controller.

For information on how to work with and install licenses, see *Managing licenses on page 15-7*.

Key concepts

All service controllers include basic Layer 2 (L2) mobility support allowing wireless users to roam between APs within the same subnet. MSM7xx Mobility Controllers include the added features WPA2 Opportunistic Key Caching and L3 Mobility.

WPA2 Opportunistic key caching

Using optimizations of 802.1X/802.11i authentication, WPA2 Opportunistic Key Caching enables a wireless client to perform a full RADIUS authentication once and then re-use those authentication credentials on each subsequent roam without the need to re-authenticate through RADIUS. The service controller maintains updated key information on APs based on the Mobility Neighborhood so that a wireless user can roam between APs without incurring a full 802.1X RADIUS handshake delay.

WPA2 Opportunistic Key Caching provides secure and fast user authentication based on the WPA2 and 802.1X standards. It:

- Eliminates delays associated with reauthentication.
- Provides hand-offs in less than 50 milliseconds, as required for time-sensitive services such as voice.
- Preserves a user's RADIUS-assigned parameters such as security and VLAN, enabling smooth transition of all services to which the user has access.

How it works

With WPA 2 Opportunistic key caching, each wireless client has one set of encryption keys that are shared by all APs in the “mobility neighborhood.” When a client roams to a new AP, it sends a PMKID (see IEEE 802.11i for more information) with its re-association request. If this PMKID matches the encryption keys for that client, then the client is able to bypass RADIUS authentication and move directly to the 4-way encryption handshake.

Note

The wireless client software must support Opportunistic Key Caching. The Microsoft windows wireless client and the Juniper Odyssey client both support this.

Layer 3 Mobility

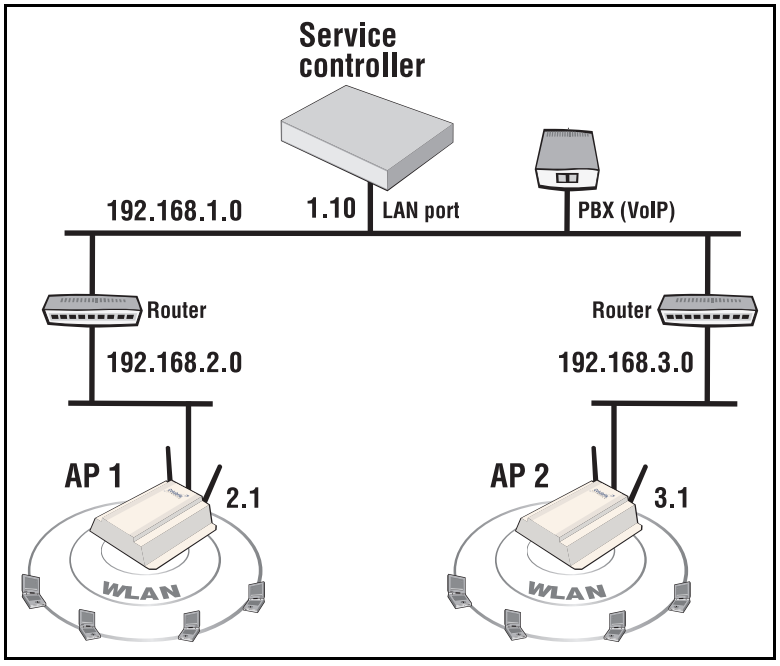
Layer 3 (L3) mobility enables users to roam between APs that are connected to different service controllers operating on different subnets, while maintaining their assigned IP address. L3 mobility enables a seamless wireless infrastructure to be deployed across a routed backbone network while delivering a consistent set of services to users, regardless of the subnets used for the underlying infrastructure. L3 mobility uses a unique technology set that eliminates the need for special client software required by some competing solutions.

How it works

The mobility feature defines a mobility domain, which is an interconnection between up to four service controllers for the purpose of exchanging mobility information on roaming users. One service controller must be defined as the primary mobility controller. It acts as the central site for distribution of mobility information. The primary controller must be reachable via the LAN port on all other service controllers that are part of the mobile domain. (Internet port connections are not supported.)

Wireless mobility scenario

This section walks you through the minimum configuration steps necessary to implement a simple mobility scenario with support for Opportunistic key caching and L3 Mobility. Once implemented, wireless clients, including Wi-Fi phones, can roam between APs on different subnets without experiencing delays as the wireless client is switched from one AP to the other. The scenario is illustrated as follows:



The following items are required to implement this scenario:

- One MSM7xx service controller such as the MSM710 Mobility Controller or MSM710 Access Controller with a user-installed Mobility license.
- Two APs such as the MSM310.
- A PBX / VoIP server.
- A voice-capable wireless client such as a Wi-Fi phone.
- Multiple subnets connected by router. This scenario uses three subnets: 192.168.1.0, 192.168.2.0, and 192.168.3.0.
- A DHCP scope defined for each subnet.

A. Configure the network

1. Using appropriate router and DHCP server configuration (beyond the scope of this guide) construct a three-subnet network as illustrated above with the service controller (LAN port) on subnet **192.168.1.0**, one MSM310 on subnet **192.168.2.0** and another on subnet **192.168.3.0**.

B. Pre-configure the service controller

The service controller LAN port defaults to IP address 192.168.1.1. You will likely need to change this address to an available address on subnet 192.168.1.0. Before connecting the service controller to your network, pre-configure its IP address as follows:

1. Reset the service controller to its factory defaults. In its management tool, select **Service Controller >> Maintenance > Config file management**. For additional information see *Appendix C: Resetting to factory defaults*.
2. Set your computer IP address to a value in the range 192.168.1.2 to 192.168.1.254.
3. Disconnect any cable from the service controller Internet port and connect the service controller LAN port to your computer.
4. In a Web browser, open page: **https://192.168.1.1**.
5. Select **Service Controller >> Network > Ports > LAN port** and under **Addressing**, set an available **Static IP address** (**192.168.1.10** in this scenario) and **Mask**. After selecting **Save**, you will lose connection with the management tool. This is expected behavior.

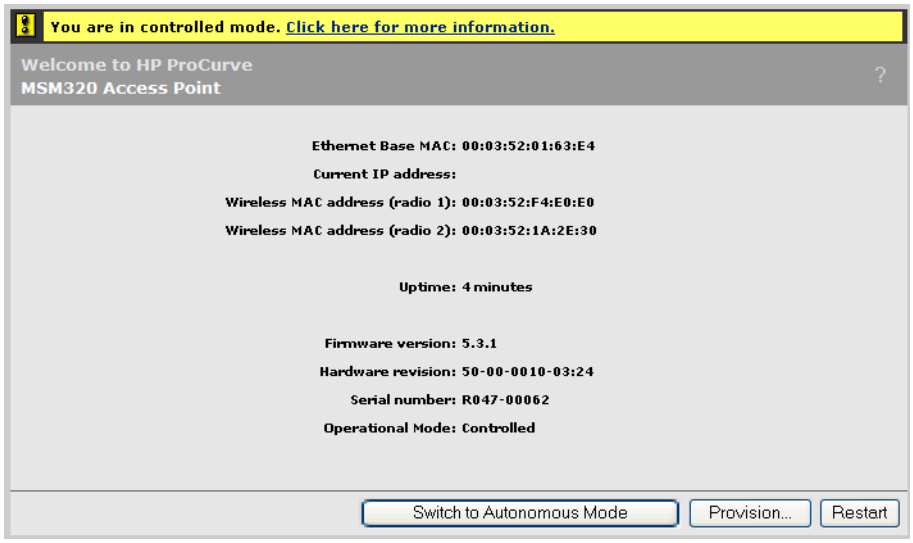
C. Connect the service controller to the network

1. Connect the service controller LAN port to the network on which it will reside (subnet 192.168.1.0).
2. Configure the LAN port on your computer for Automatic IP address assignment by DHCP and connect it to the same 192.168.1.0 subnet.
3. In a Web browser open page **https://**<IP address of the service controller> (**192.168.1.10** in this scenario). Confirm that the management tool opens. This is sufficient to prove that the service controller is reachable on the network via its LAN port.

D. Provision the APs

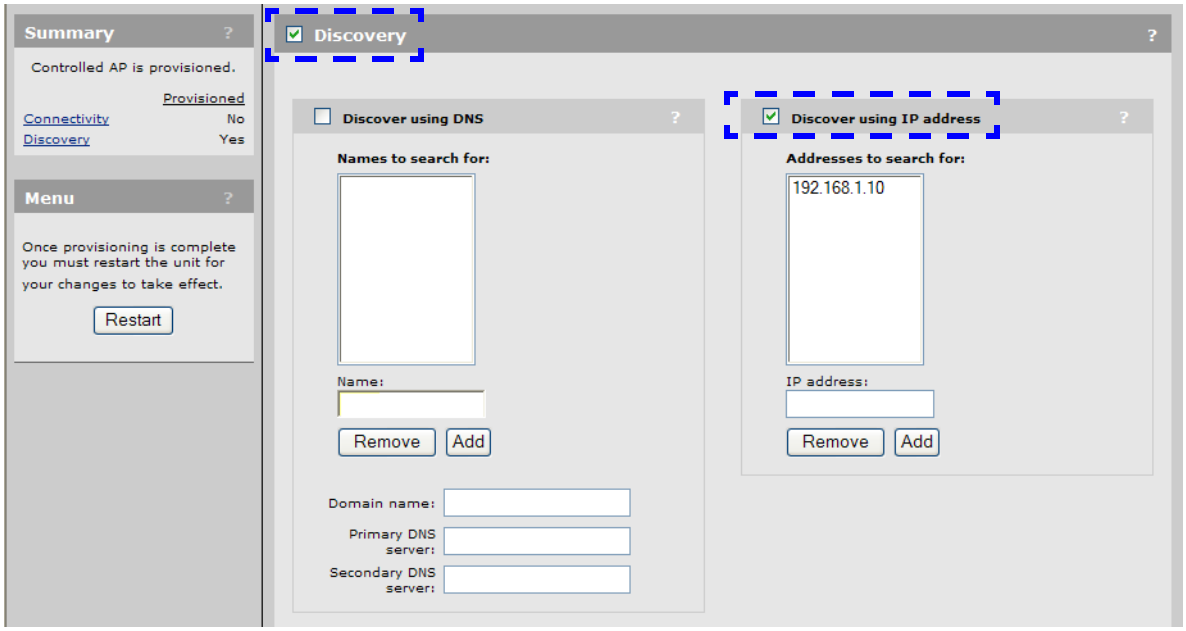
The two APs need to be provisioned so that they can find the service controller that will manage them across the routers. Before connecting the APs to the network, provision each one as follows:

1. Reset the AP to its factory default state: Power-on the AP without any Ethernet cables connected, and press and hold the Reset switch until the status lights blink three times. See *Resetting to factory defaults* in the *MSM3xx / MSM4xx Management and Configuration Guide*.
2. Using a crossover cable, connect your computer to Port 1 on the AP.
3. With your computer connected to the same subnet as the AP, open the AP management tool In a Web browser at **https://192.168.1.1**. The controlled mode home page opens.



4. Select **Provision** at the bottom of the home page and then select the **Discovery** tab. (The **Provision** button is only available if the AP is in its factory-default state.)

5. Select the **Discovery** and **Discover using IP address** check boxes.



6. Under IP address specify the IP address of the service controller configured in step B 5 above (**192.168.1.10** in this scenario) and select **Add.** Select **Save**.

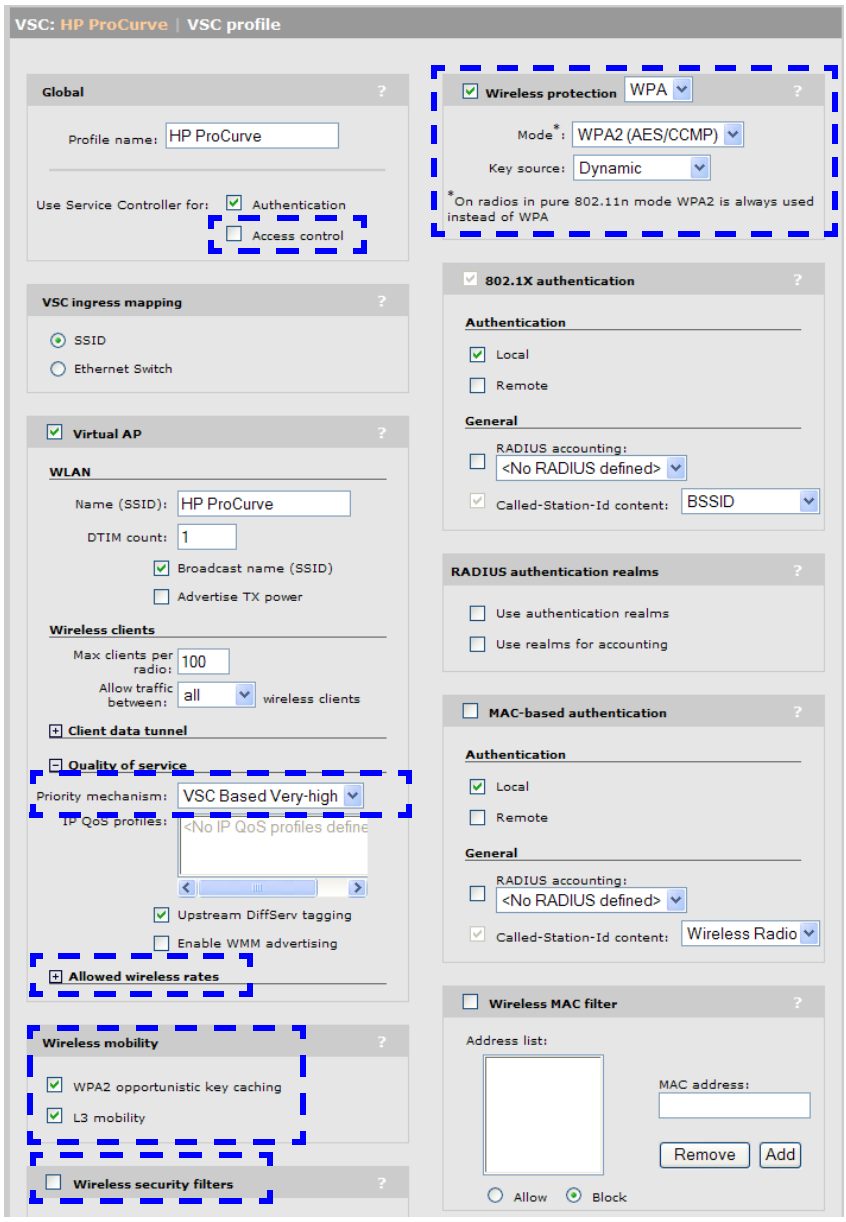
Both APs are now provisioned to find the service controller across the routers.

E. Connect each AP to its subnet

1. Connect Port 1 of AP 1 to subnet 192.168.2.0 and connect Port 1 of AP 2 to subnet 192.168.3.0.
2. In the service controller management tool, verify that both APs get discovered by the service controller.
3. For testing purposes ensure that the two APs are as far apart as possible but no more than 100 feet (31 meters).

F. Configure a VSC profile

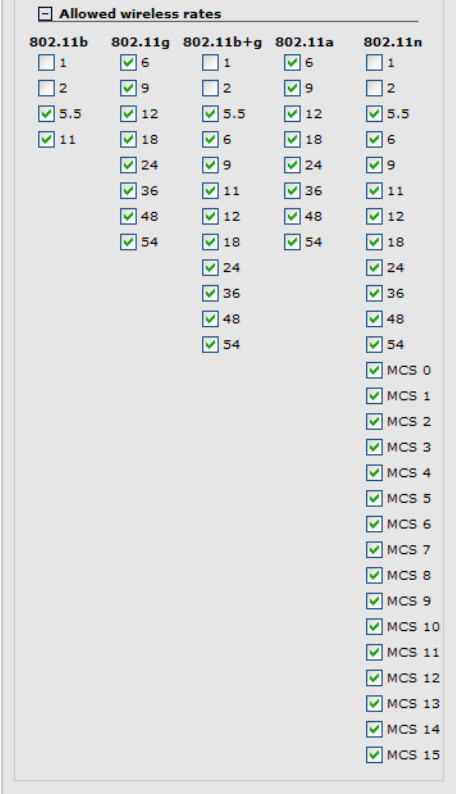
1. In the service controller management tool, open the VSC profile that you will use for mobility, and configure the following highlighted items as described below:



   For details on each option, see the online help.

2. Under **Global**, clear **Access control**.
3. Select **Wireless protection** and configure its options as follows:
   a. Set Wireless protection to **WPA.**
   b. Set **Mode** to **WPA2 (AES/CCMP)**.
   c. Set **Key source** to **Dynamic**.

4. Under **Virtual AP: Quality of service**, configure the following:
   a. Set **Priority mechanism** to **VSC Based Very-high**. This is important for voice services.
   b. Unless your network requires it, clear **Upstream DiffServ tagging**.
   c. Unless your Wi-Fi phones specifically support Wi-Fi Multimedia, clear **Enable WMM advertising**.
5. Under **Virtual AP: Allowed wireless rates**, clear all speeds below 5.5 Mbps.



6. Under **Wireless mobility**, select **WPA2 opportunistic key caching** and **L3 mobility**.

Note

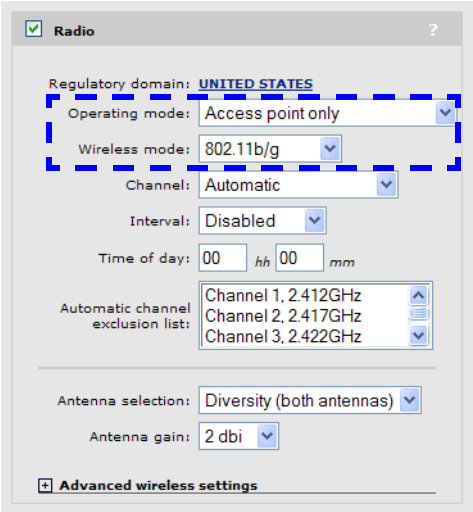
If the Wi-Fi phones that you will use support only pre-shared key static encryption (Spectralink for example), do not enable **WPA2 opportunistic key caching**.

7. Clear **Wireless security filters**.

G. Configure the radios

Configure the radios of both APs as indicated here.

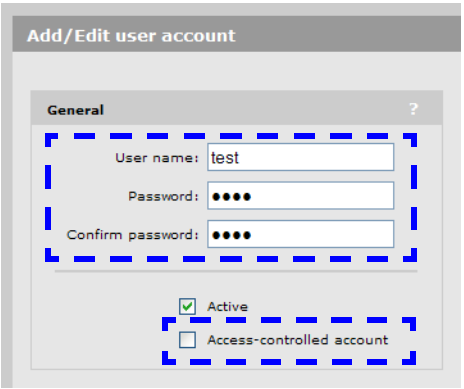
1. Select **Service Controller > Controlled APs >> Configuration > Radio list**, select a product and configure the following highlighted items (sample shown for MSM310):



2. Set **Operating mode** to **Access point only**.
3. Set **Wireless mode** according to phone type. It is recommended that you select **802.11b/g** even if your phones only support 802.11b.

H. Add a user

1. On page **Service Controller >> Users > User Accounts**, add a test user as highlighted:



2. Under **General**, fill in **User name**, and **Password**.
3. Clear **Access-controlled account**.

I. Test with a Wi-Fi phone

You can follow these basic steps to test your Mobility network with a Wi-Fi phone.

If you enabled **WPA2 Opportunistic Key Caching** in step **F.6** above, test with a Wi-Fi phone that supports this such as the **Hitachi WIP-5000-EA**.

Otherwise, test with a Wi-Fi phone that supports pre-shared key (static encryption).

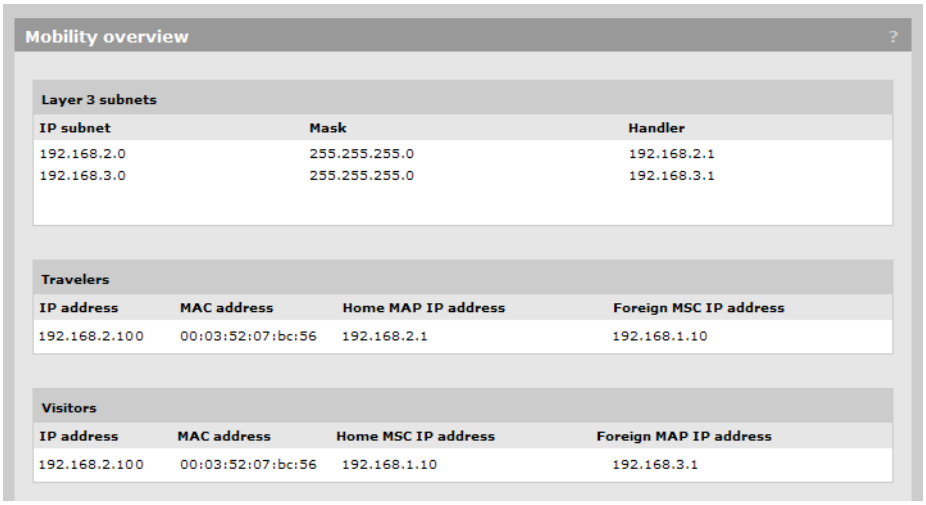
1. Configure your Wi-Fi phone to use wireless network “Corporate” and user “test”. If applicable, configure the phone to use **WPA2 Opportunistic Key Caching**.
2. Although the network is set up to assign an IP address to the phone via DHCP you may wish to initially assign a static IP address to the phone. Be sure to assign an available address outside of the range of addresses being assigned by the DHCP server.
3. Position yourself as far away as possible from the second AP (AP 2) but within good range of the first AP (AP 1).
4. Initiate a voice call and commence a conversation with someone.
5. Move away from AP 1 and close to AP 2 to force roaming, while continuing to talk (or listen).

Note

If the APs are close together (a few feet / meters apart) you can still force roaming by manipulating the antennas. Initially connect one antenna to AP 1 and no antenna to AP 2. Begin a voice call via AP 1 and then attach one antenna to AP 2. Then, remove the antenna from AP 1 to force the roam to AP 2.

6. Confirm that the phone call is not interrupted during the hand off from AP 1 to AP 2.
7. If you wish, return to the original AP while continuing to talk, again confirming smooth hand off back to AP 1.

In the service controller management tool you can see with which AP a particular wireless client is associated. Open page **Service Controller > Controlled APs >> Overview > Wireless client** and look for the MAC address of the Wi-Fi phone you are testing. You can view L3 mobility information on page **Service Controller >> Status > L3 mobility**.



The previous sample L3 mobility status page shows how it looks after the Wi-Fi phone (IP address 192.168.2.100) has roamed from its home AP (AP 1 at 192.168.2.1) to the foreign AP (AP 2 at 192.168.3.1). The phone IP address of 192.168.2.100 is retained when it roams to AP 2. The service controller uses IP address 192.168.1.10, and since there is only one service controller, both the Home and Foreign addresses are the same.

12

Working with VPNs

Contents

Overview 12-2

Securing wireless client sessions with VPNs 12-3
- Configure an IPSec profile for wireless client VPN 12-4
- Configure L2TP server for wireless client VPN 12-5
- Configure PPTP server for wireless client VPN 12-5
- VPN address pool 12-6

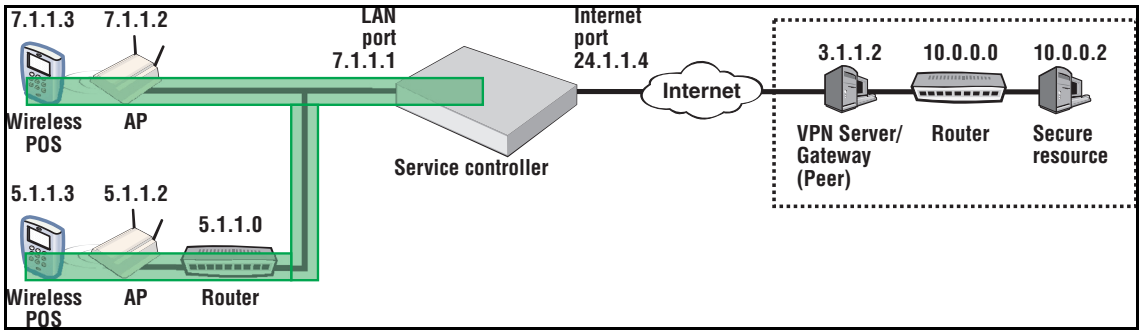
Securing service controller communications to remote VPN servers 12-7
- Configure an IPSec policy for a remote VPN server 12-8
- Configure PPTP client for a remote VPN server 12-9
- Keeping user traffic out of the VPN tunnel 12-11

Additional IPSec configuration 12-11
- IPSec VLAN mapping 12-12
- Local group list 12-12
- IPSec security policy database 12-12

Overview

Virtual private networks (VPNs) create secure tunnels across non-secure infrastructure such as the Internet or publicly-accessible networks. The service controller features virtual private network (VPN) capabilities that enable it to do the following:

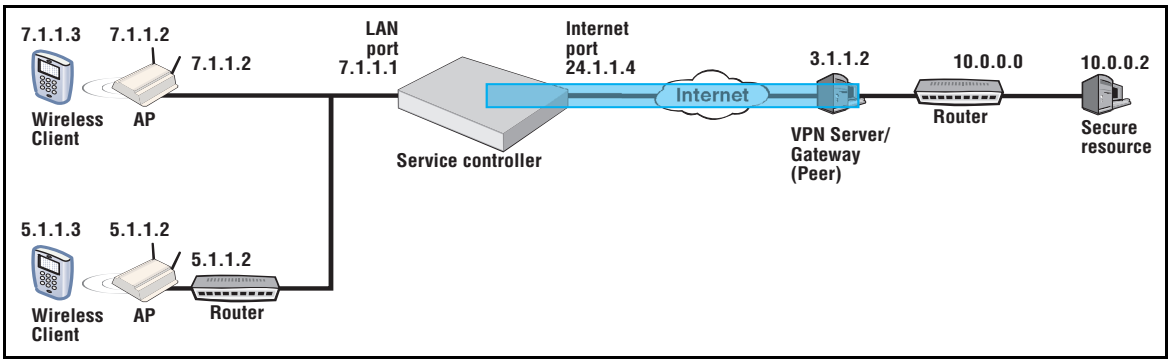
- Secure wireless client sessions with a VPN tunnel between wireless clients such as wireless point-of-sale (POS) terminals and the service controller. IPSec, L2TP, and PPTP are all supported. (VPN tunnel represented in green.)



Note

For WPA-capable wireless clients, a better alternative to VPNs, is to extend WPA termination from the AP to the service controller. See *Terminate WPA at the service controller on page 2-14*.

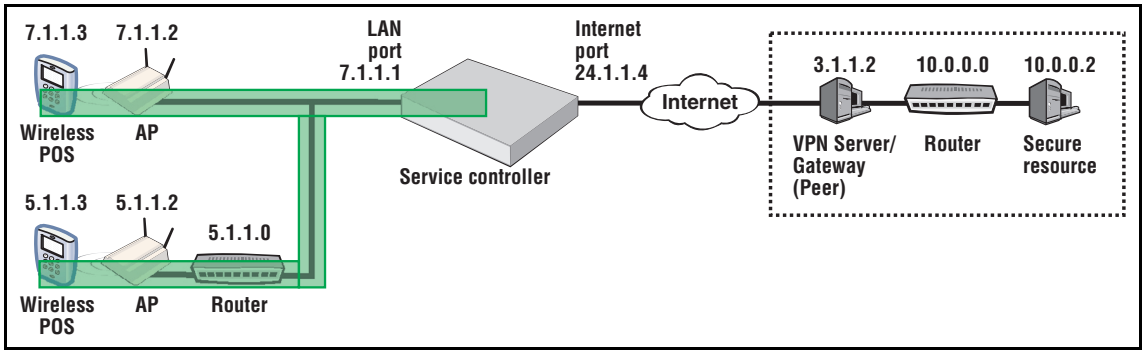
- Secure service controller communications to VPN servers, including both management and client traffic. For example, the service controller can securely contact a remote RADIUS server for user authentication. IPsec and PPTP are supported. (VPN tunnel represented in blue.)



Securing wireless client sessions with VPNs

Note The ability to secure wireless client sessions is intended for low-data-volume applications like that of wireless POS terminals.

To secure wireless client sessions, create a VPN tunnel from the wireless client to the service controller. The sample topology seen earlier serves as an example for the sample configurations that follow. In this example, the service controller LAN port has an IP address of 7.1.1.1, the APs are at 7.1.1.2 and 5.1.1.2, and the wireless POS are at 7.1.1.3 and 5.1.1.3.



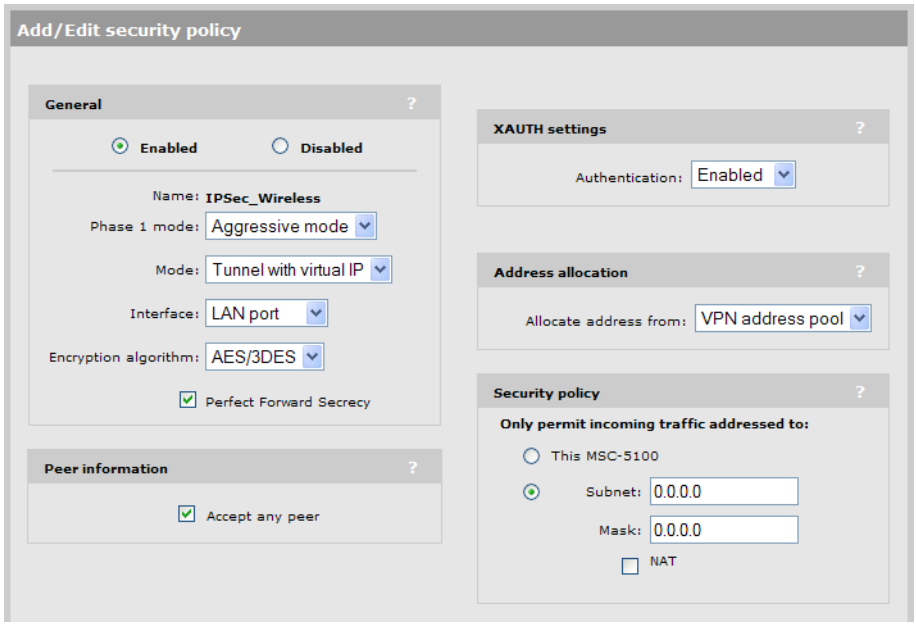
To use VPNs to secure wireless client sessions, configure an IPSec policy for this purpose, or configure the L2TP server or PPTP server.

Note Wireless clients are typically assigned IP addresses from the VPN address pool. Configure this first via **Service Controller >> Network > Address allocation > VPN address pool**. See *VPN address pool on page 12-6*.

Note Wireless clients require VPN software that is configured to work with your VPN configuration on the service controller.

Configure an IPSec profile for wireless client VPN

1. On page **Service Controller > VPN > IPSec** select **Add Policy**, and define a policy similar to this:



Note the selections made in the sample **Add/Edit security policy** page above.

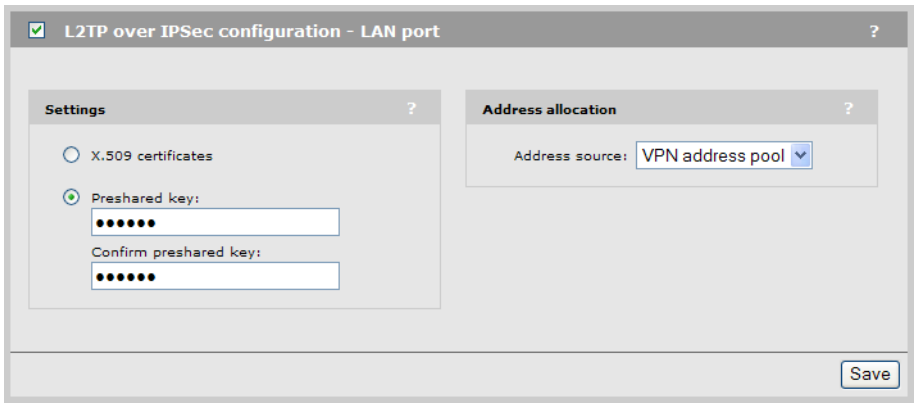
Option	Value to set	Notes
General	Enabled	
Name	user-defined	
Phase 1 mode	**Aggressive mode**	Aggressive mode requires that a group be configured. See *Local group list on page 12-12*.
Mode	**Tunnel with Virtual IP**	Allows IP addresses to be assigned to the wireless clients.
Interface	**LAN port**	
Encryption algorithm	Select as desired	
Perfect Forward Secrecy	Leave enabled	
Accept any peer	Enabled	Accepts any wireless client.
XAUTH > Authentication	Enabled	
Allocate address from	**VPN address pool**	First define address pool on **Network > Address allocation**.

Option	Value to set	Notes
Security policy	Subnet and Mask of **0.0.0.0**	A Subnet and Mask of 0.0.0.0. causes all wireless traffic between the client and the service controller to be accepted.

See the online help for option descriptions.

Configure L2TP server for wireless client VPN

1. On page **Service Controller >> VPN > L2TP server** enable **L2TP over IPSec configuration- LAN port**.



2. Either select X.509 certificates and install an X.509 security certificate (see *IPSec certificates on page 5-12*), or specify a **Preshared key**.

Note

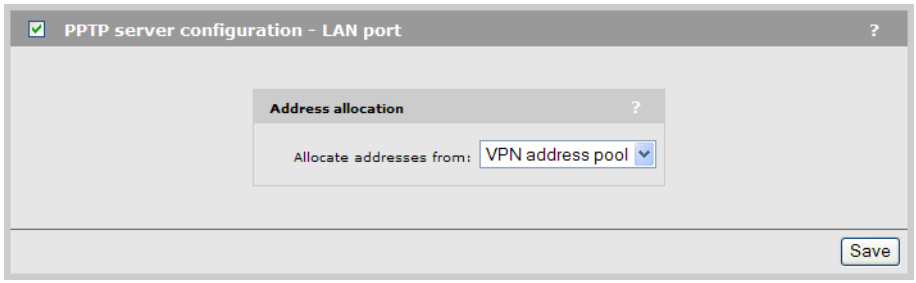
The VPN client running on the wireless device must also be configured with a matching X.509 certificate, or the **Preshared key** specified here.

3. Set **Address source** to **VPN address pool**.

   See the online help for option descriptions.

Configure PPTP server for wireless client VPN

1. On page **Service Controller >> VPN > PPTP server** enable **PPTP server configuration - LAN port**.

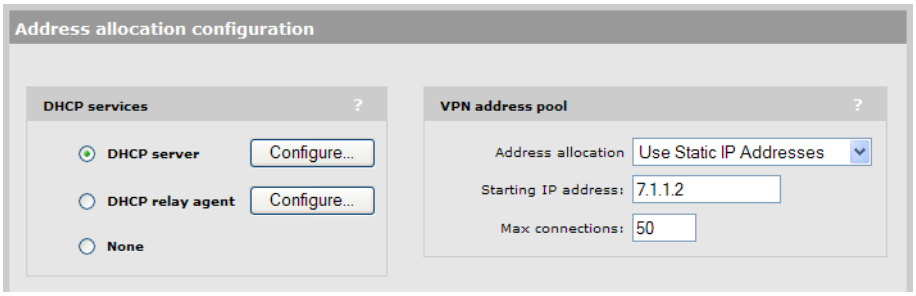


2. Set **Address source** to **VPN address pool**. See the online help for option descriptions.

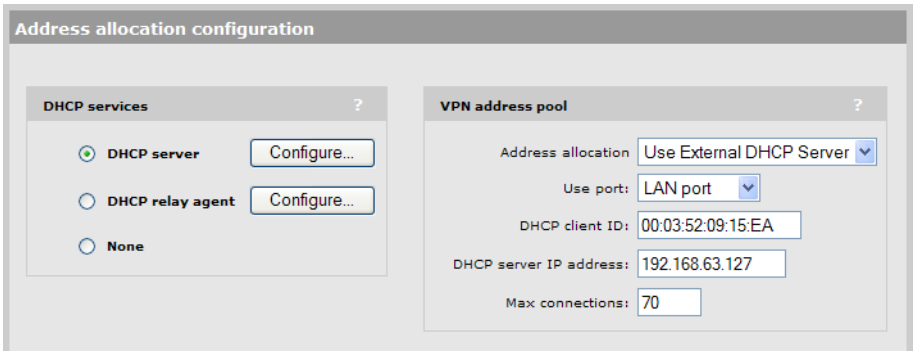
VPN address pool

When securing wireless client sessions with VPNs, it is typically necessary to provide an IP address to each client. To define a pool of addresses for this purpose, follow this procedure.

1. Select **Network > Address allocation**.
2. In **VPN address pool**, for **Address allocation** select either **Use static IP addresses** or **Use external DHCP server**.
   - For **Use static IP addresses**, define a sequential pool of addresses by specifying the **Starting IP address** and **Max connections**. For example a Starting IP address of 7.1.1.2 and a Max connections of 50, will yield a pool of IP addresses in the range 7.1.1.2 through 7.1.1.51.



   - For **Use external DHCP server**, specify settings that correspond to your external DHCP server configuration. Set **Use port** to the service controller port that will send out DHCP requests.



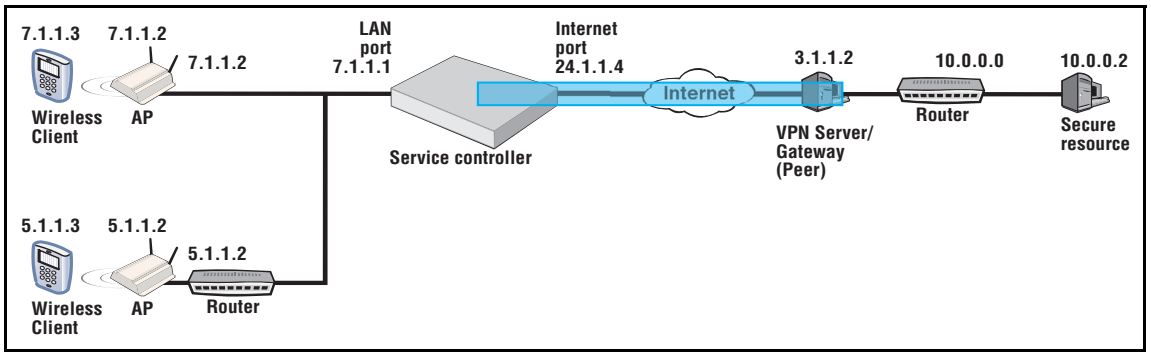
3. Select **Save**.

   See the online help for option descriptions.

Securing service controller communications to remote VPN servers

To secure the communications between the service controller and remote VPN servers, create a VPN tunnel from the service controller to the remote VPN server.

The sample topology seen earlier serves as an example for the sample configurations that follow. In this example, the service controller Internet port has an IP address of 21.1.14, the remote VPN server is at 3.1.1.2, and the secure resource is at 10.0.0.2.



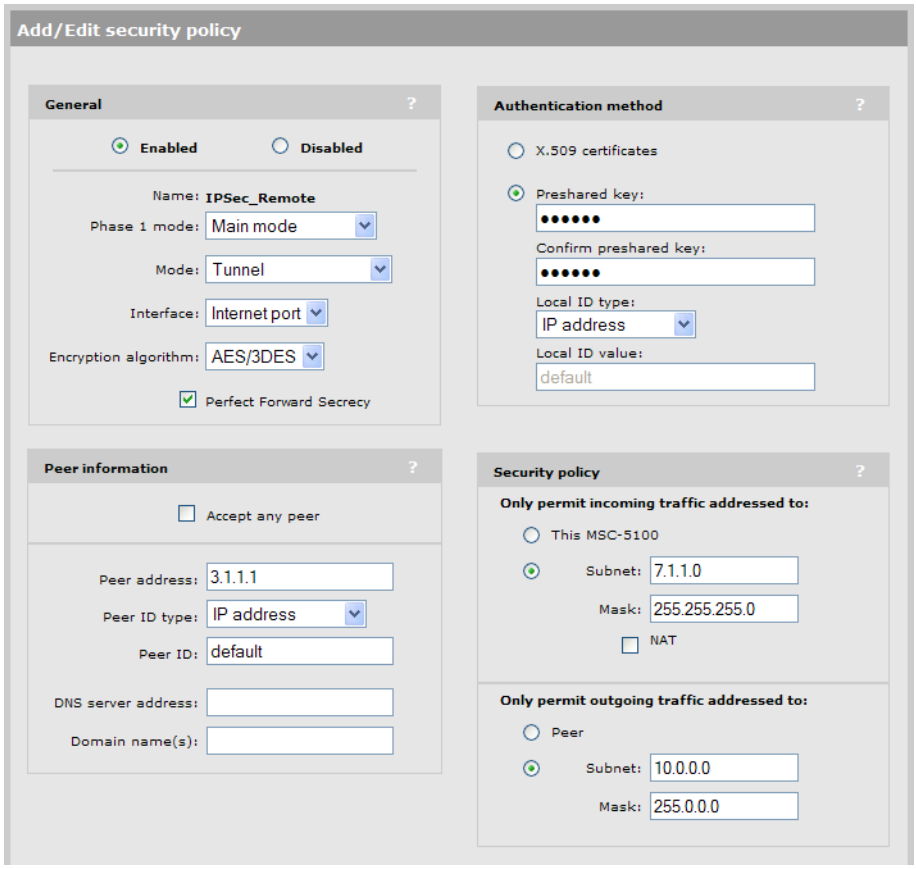
Create a VPN tunnel like this either by configuring an IPSec policy or configuring the PPTP client.

Caution

The VPN tunnel should not be used to transport user traffic. The tunnel should only be used to carry management traffic (RADIUS, SNMP, and management sessions). See *Keeping user traffic out of the VPN tunnel on page 12-11*.

Configure an IPSec policy for a remote VPN server

1. On page **Service Controller > VPN > IPSec** select **Add New Policy** and define a policy similar to this, substituting your own IP addresses:



Note the selections made in the sample **Add/Edit security policy** page above.

Option	Value to set	Notes
General	Enabled	
Name	user-defined	
Phase 1 mode	**Main mode**	
Mode	**Tunnel**	
Interface	**Internet port**	
Encryption algorithm	Select as desired	
Perfect Forward Secrecy	Leave enabled	
Accept any peer	Disabled	

Option	Value to set	Notes
Peer information	User-defined	Set according to VPN server needs. In this example, the VPN server address is 3.1.1.1.
Authentication method	User-defined	Set according to VPN server needs. Either the X.509 certificates or the Preshared key must match server configuration.
Security policy > Only permit incoming...	Identify the subnet	Identify the local subnet for which you wish to filter traffic, for example, 7.1.1.0. This must match the value defined in the policy on the peer (VPN server).
Only permit outgoing...	Identify the remote subnet	Identify the remote subnet for which you wish to filter traffic, for example, 10.0.0.0. This must match the value defined in the policy on the peer (VPN server).

See the online help for option descriptions.

See also, *Keeping user traffic out of the VPN tunnel on page 12-11*.

Configure PPTP client for a remote VPN server

Configure the PPTP client for the service controller VPN client capability via the **VPN > PPTP client** menu.

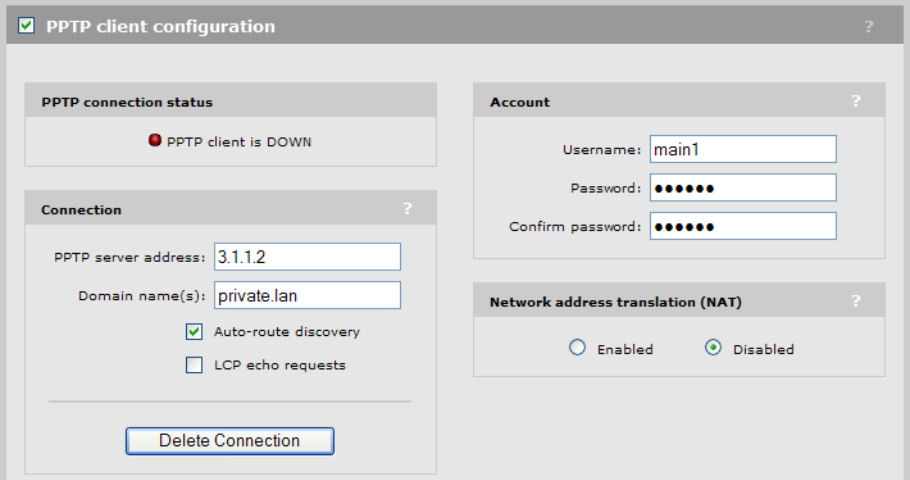
The PPTP client enables the service controller to create a secure tunnel to any device that provides a PPTP server. All traffic sent though this tunnel is protected against eavesdropping by means of encryption.

Note

The PPTP tunnel should not be used to transport user traffic. To prevent user traffic from entering the tunnel, you must define access list definitions to DENY access to all subnets on the other side of the tunnel. The tunnel should be used to carry management traffic only (RADIUS, SNMP, management sessions). See *Keeping user traffic out of the VPN tunnel on page 12-11*.

Configuration

To view and configure the PPTP client, select **Service Controller >> VPN > PPTP client**. The PPTP client is disabled by default.



Connection

PPTP server address

Specify the domain name or IP address of the PPTP server the service controller will connect to.

Domain name(s)

Specify the domain name(s) that are reachable through the tunnel. Put a space between each name as a separator. The service controller routes all traffic addressed to this domain through the PPTP connection. If you do not want to enter a Domain name, enter **private.lan** instead.

Auto-route discovery

Enable this option if you want the service controller to automatically discover and add routes to IP addresses on the other side of the PPTP tunnel. The addresses must be part of the specified domain. Routes are added only when an attempt is made to access the addresses.

LCP echo requests

Certain VPN servers may terminate your connection if it is idle. If you enable this option, the service controller will send a packet from time to time to keep the connection alive.

Account

Username

Specify the username the service controller will use to log on to the PPTP server. If you are logging on to a Windows XP domain, specify **domain_name\username**

Password / Confirm password

Specify the password the service controller will use to log on to the PPTP server.

Network Address Translation (NAT)

If you enable NAT, it effectively hides the addresses of all local computers so that they are not visible on the other side of the PPTP connection.

If you disable NAT, then the appropriate IP routes must be added to send traffic through the tunnel.

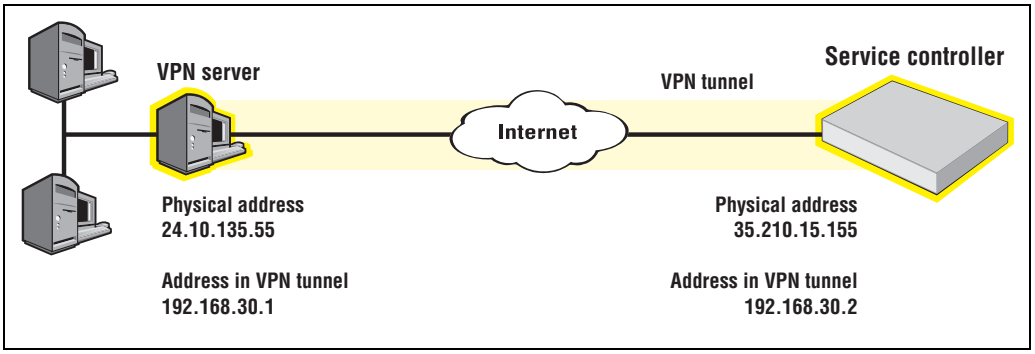
Keeping user traffic out of the VPN tunnel

Note

The VPN tunnel should not be used to transport user traffic. The tunnel should only be used to carry management traffic (RADIUS, SNMP, and management sessions).

To prevent user traffic from entering the tunnel, you must define access list definitions to DENY access to all subnets on the other side of the tunnel.

Consider the following scenario:



To protect the VPN, add the following definitions to the site access list:

```
access-list=vpn,DENY,all,192.168.30.0/24,all
use-access-list=vpn
```

This definition applies to all users, whether they are authenticated or not. It blocks access to the VPN subnet for all traffic. For more information on using the access list feature, see *Access list on page 9-30*.

Additional IPSec configuration

Page **Service Controller > VPN > IPSec** provides some additional configuration options and information.

For information about the IPsec certificates see *IPSec certificates on page 5-12*.

IPSec VLAN mapping

Use these settings to define how IPSec traffic is routed on the LAN and Internet ports. You can assign traffic to the untagged interface (no VLAN) or to any defined VLAN.

Local group list

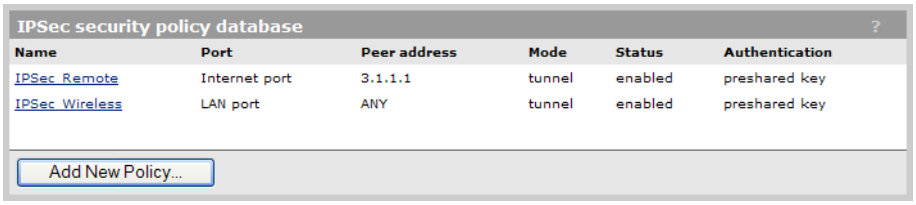
When using IPSec aggressive mode, groups can be used to authenticate IPSec connections from clients (peers). The client must supply the group name matching one of the groups defined here to establish a security association with the service controller.

Create all needed groups, providing information as follows:

- Group name: Group names are case-sensitive and should be in the format user@FQDN.com or FQDN.com. For example, fred@mycompany.com or server99.mycompany.com.
- Password/Confirm password: Passwords must be at least six characters long and contain at least four different characters.

IPSec security policy database

The **IPSec security policy database** table shows all the IPSec security policies that are defined on the service controller. A security policy defines the criteria that must be met for a peer to establish an IPSec security association (SA) with the service controller.



This information is provided:

- **Name**: Name assigned to the security policy.
- **Port**: Port assigned to the security policy.
- **Peer address**: Address of the peer which can establish an SA using this policy.
- **Mode**: Indicates the IPSec mode (tunnel or transport) supported by this policy.
- **Status**: Indicates whether the policy has been enabled. An SA can only be established when a policy is enabled.
- **Authentication**: Indicates the method used to authenticate peers.

13

Local mesh

Contents

Introduction 13-2

Local mesh terminology 13-3

Local mesh operational modes 13-4

Node discovery 13-4

Operating channel 13-5

Local mesh profiles 13-5
- Configuration guidelines 13-6
- Configuring a standard profile 13-7
- Other configuration settings 13-9

Provisioning local mesh links 13-12

Sample local mesh deployments 13-15
- RF extension 13-15
- Building-to-building connection 13-15
- Dynamic network 13-16

Introduction

Note

Local mesh support is available for both controlled and autonomous APs.

The local mesh feature replaces the need for Ethernet cabling between APs, enabling expanded Wi-Fi coverage through the use of wireless bridges to transport network traffic in hard-to-wire or outdoor areas.

Key local mesh features include:

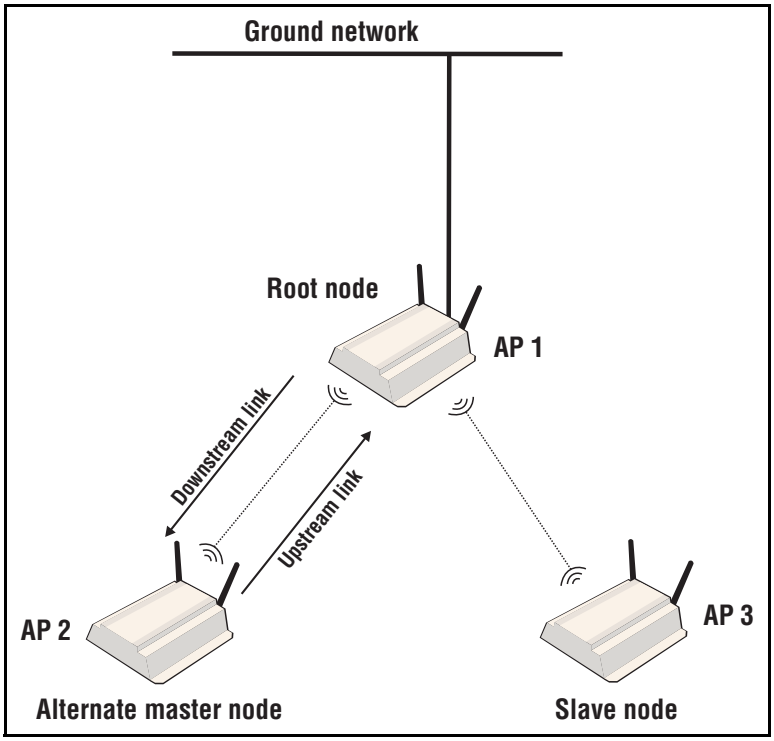
- **Automatic link establishment:** Nodes automatically establish wireless links to create a full-connected network. A dynamic network identifier (local mesh group ID) restricts connectivity to groups of nodes, enabling distinct groups to be created with nodes in the same physical area.
- **Provides fall-back operation to recover from node failure.** In a properly designed implementation, redundant paths can be provided. If a node fails, the mesh will automatically reconfigure itself to maintain connectivity.
- **Maintains network integrity when using DFS channels.** In accordance with the 802.11h standard, dynamic frequency selection (DFS) detects the presence of certain radar devices on a channel and automatically switches the network node to another channel if such signals are detected. 802.11h is intended to resolve interference issues with military radar systems and medical devices.

Note

Depending on the radio regulations of some countries, DFS channels are only available on the 802.11a band, which is the preferred band for local mesh backhaul. If more than one node detects radar simultaneously and must switch channels, each node does not necessarily switch to the same channel, and the network might never reconverge. To avoid this problem, local mesh detects a change in channel and provides a means to reconnect on other channels by scanning on multiple channels. See *Operating channel on page 13-5*.

Local mesh terminology

The following table defines terms that are used in this guide when discussing the local mesh feature.



Term	Definition
Node	An AP that is configured to support local mesh connections.
Root node	The root node is configured in **Master** mode and provides access to the ground network.
Alternate master node	A node that is configured in **Alternate master** mode which enables it to make upstream and downstream connections.
Slave node	A node that is configured in **Slave** mode which enables it to make upstream connections only.
Ground network	Wired network to which the root node is connected. This is the network to which the local mesh provides access for all connected alternate master and slave nodes.
Mesh	A series of nodes that connect to form a network. Each mesh is identified by a unique mesh ID.
Link	The wireless connection between two nodes.
Downstream link	A link that transports data away from the ground network.

Term	Definition
Upstream link	A link that transports data towards the ground network.
Peer	Any two connected nodes are peers. In the diagram, *AP 1* is *the peer of both AP 2 and AP 3*.

Local mesh operational modes

Three different roles can be assigned to a local mesh node: **Master, Alternate Master,** or **Slave.** Each role governs how upstream and downstream links are established by the node.

- **Master**: Root node that provides the upstream link to the *ground network* that the other nodes want to reach. The master never tries to connect to any other node. It waits for links from downstream alternate master or slave nodes.

Note

It is possible to have several masters for the same mesh ID connected to the ground network. This can be used to provide redundant paths to the ground network for downstream nodes.

- **Alternate Master**: First establishes an upstream link with a master or alternate master node. Next, operates as a master node waiting for links from downstream alternate master or slave nodes.
- **Slave**: Can only establish an upstream link with master or alternate master node. Slave nodes cannot establish downstream links with other nodes.

Node discovery

Discovery of another node to link with is limited to nodes with the same mesh ID. The link is established with the node that has the best score based on the following calculation:

```
Score = SNR - (Number of hops x SNR cost of each hop)
```

If a node looses its upstream link, it automatically discovers and connects to another available node.

Note

A master or alternate master must be seen with an SNR of 20 or higher before a slave will attempt to connect to it.

Operating channel

If a mesh operates on a dynamic frequency selection (DFS) channel, the master node selects the operating channel. If another node detects radar and switches channels, that node reports the channel switch to the master node, which initiates a channel switch for the nodes connected to it. This allows the local mesh to converge on a specific channel.

A node that uses a DFS channel and that loses connection with its master, scans channels to find a master on another channel, which can be a new master or the same master.

If the local mesh does not operate on a DFS channel, configure the radios in one of the following ways:

- Configure the radios on all nodes to use the same fixed channel.
- Configure the radios for automatic channel selection. In this case the master selects the least noisy channel. Slaves and alternate masters scan channels until they find the master, then tune to the master channel and link with the master.

Local mesh profiles

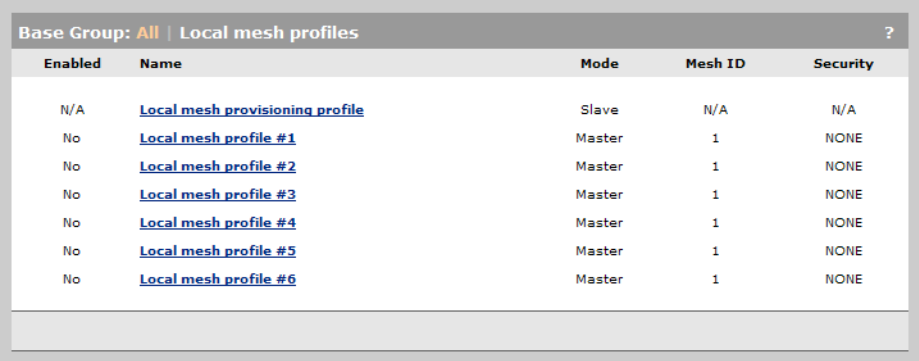
A local mesh profile defines the characteristics for the type of links that can be established with other nodes as follows:

Role	Upstream link	Downstream link
Master	None.	Up to nine links with alternate master or slave nodes.
Alternate master	A single link to a master node or alternate master node.	Up to eight links with alternate master or slave nodes.
Slave	A single link to a master node or alternate master node.	None.

Each node supports up to six profiles plus one provisioning profile. When a profile is active, a node constantly scans and tries to establish links as defined by the profile.

The **local mesh provisioning profile** is used by the wireless link created on a provisioned AP to support discovery of the service controller. Initially, this link operates in slave mode. If you configure this profile as an alternate master, then it can also be used to establish up to nine downstream links with alternate master or slave nodes. See *Provisioning local mesh links on page 13-12* for more information.

Local mesh profiles are configurable at the controlled APs, group, or AP level. To view all profiles select **Service Controller > Controlled APs >> Configuration > Local mesh**. Or you can expand **Controlled APs** and select a group or specific AP. The following is an example of the profile list displayed when selecting **Controlled APs >> Configuration > Local mesh**.

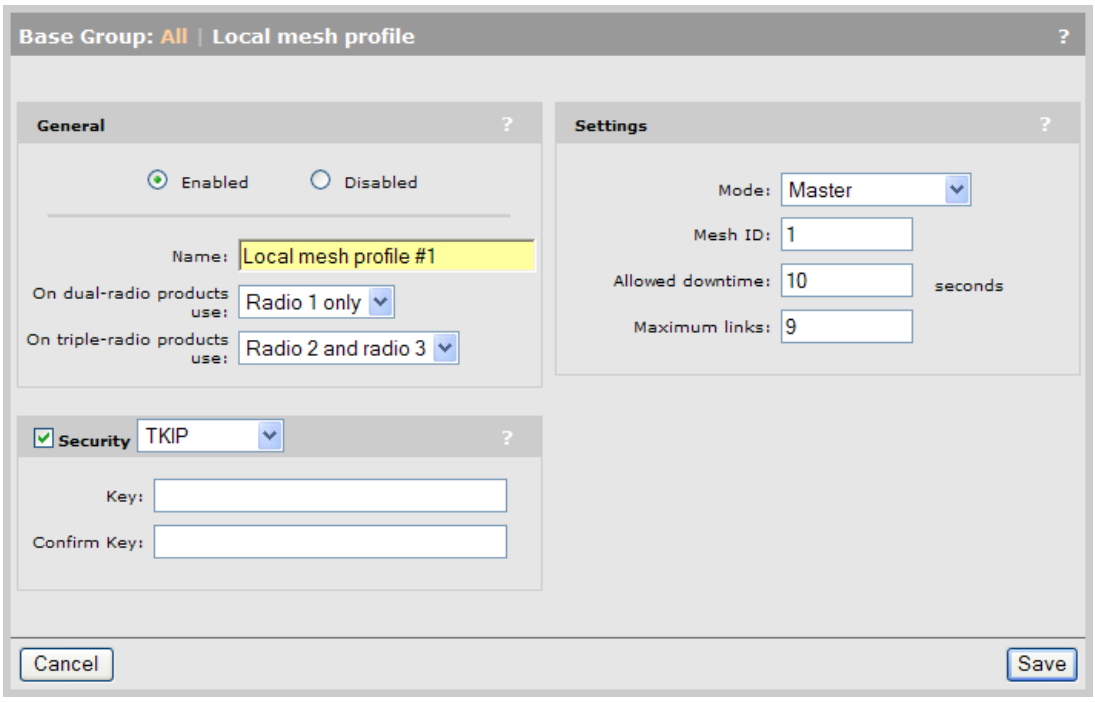


Configuration guidelines

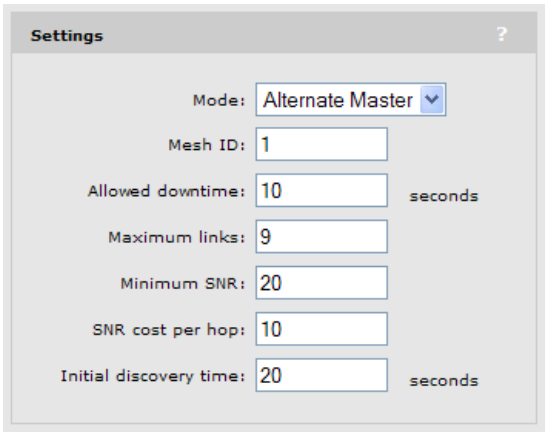
- In addition to the provisioning profile, you can configure a total of six local mesh profiles on each node.
- Each local mesh profile (on a master or alternate master) can be used to establish up to nine links with other nodes.
- The same security settings must be used on all nodes in the same mesh.
- Any node that reaches the service controller through the local mesh and uses local mesh itself, must be provisioned prior to discovery.
- Daisy-chaining of nodes using local mesh links dramatically reduces throughput (which is typically divided by two for each hop) especially when one or more of the following are true:
  - Nodes provide both upstream and downstream links on the same radio.
  - Nodes share a radio with AP functionality.
  - IP traffic originating from a node can be sent on the link on which the service controller was discovered.

Configuring a standard profile

To configure profiles #1 to #6, select a name in the list. The **Local mesh profile** page opens.



For **Slave** and **Alternate Master**, the **Settings** box shows the additional options, for example Alternate Master:



General

Enabled/Disabled

Specify if the profile is enabled or disabled. The profile is only active when enabled.

Name

Name of the profile.

On dual-radio products use

Select the radio to use for this link.

Settings

Mode

Three different roles can be assigned to a node: master, alternate master, or slave. Each role governs how links are established. Links are defined as either upstream or downstream.

- **Master:** The master is the root node that provides the upstream connection to the *ground network* that the other nodes want to reach. The master will only create downstream local mesh links to alternate master or slave nodes.
- **Slave:** Slave nodes can only establish upstream links with master or alternate master nodes. Slave nodes cannot establish downstream links with other nodes.
- **Alternate Master:** An alternate master node must first establish an upstream link with a master or alternate master node before it can establish downstream connections with an alternate master or slave node.

Mesh ID

Unique number that identifies a series of nodes that can connect together to form a local mesh network.

Allowed downtime

The maximum time (in seconds) that a link can remain idle before the link actually gets deleted. When a slave (or alternate master) looses its link to its master, the discovery phase is re-initiated.

Minimum SNR

(Alternate master or slave nodes)

This node will only connect with other nodes whose SNR is above this setting (in dB).

SNR cost per hop

(Alternate master or slave nodes)

This value is an estimate of the cost of a hop in terms of SNR. It indicates how much SNR a node is willing to sacrifice to connect to node one hop closer to the root node, because each hop has an impact on performance, especially when using a single radio.

Initial discovery time

(Alternate master or slave nodes)

Amount of time that will be taken to discover the best available master node. The goal of this setting is to delay discovery until all the nodes in the surrounding area have had time to startup, making the identification of the best master more accurate. If this period is too short, a slave may connect to the first master it finds, not necessarily the best.

Security

Enable this option to secure data transmitted on the wireless link. The APs on both sides of the wireless link must be configured with the same security options.

WEP

Enables WEP to secure traffic on the wireless link.

Specify the encryption key the node will use to encrypt/decrypt all data it sends and receives. The key is 128 bits long and must be specified as 26 hexadecimal digits.

TKIP

Enables TKIP encryption to secure traffic on the wireless link.

The node uses the key you specify in the PSK field to generate the TKIP keys that encrypt the wireless data stream.

Specify a key that is between 8 and 63 ASCII characters in length. It is recommended that the key be at least 20 characters long, and be a mix of letters and numbers.

AES/CCMP

Enables AES with CCMP encryption to secure traffic on the wireless link. This is the most secure method.

The node uses the key you specify in the PSK field to generate the keys that encrypt the wireless data stream.

Specify a key that is between 8 and 63 ASCII characters in length. It is recommended that the key be at least 20 characters long and be a mix of letters and numbers.

Other configuration settings

Single radio vs. dual radios

Simultaneous AP and local mesh

A radio can be configured to simultaneously support wireless clients and the creation of one or more local meshes. Although this offers flexibility it does have several limitations as follows:

- It reduces overall throughput since the total available bandwidth is shared between the local meshes and wireless users.
- It limits you to using the same radio options for both wireless clients and local meshes.

A more effective way to handle this is to use a multi-radio AP. This allows one radio to be dedicated for wireless users and another for local mesh. Each radio can be configured optimally according to its application.

Using two radios for local mesh

Two radios can be enabled at the same time on a local mesh profile. This enables the node to search for a master (or alternate master) on both radios. Once a master is found and the link is established on one radio, the other is used to create downstream links. This greatly improves throughput over single-radio deployments.

Using 802.11a for local mesh

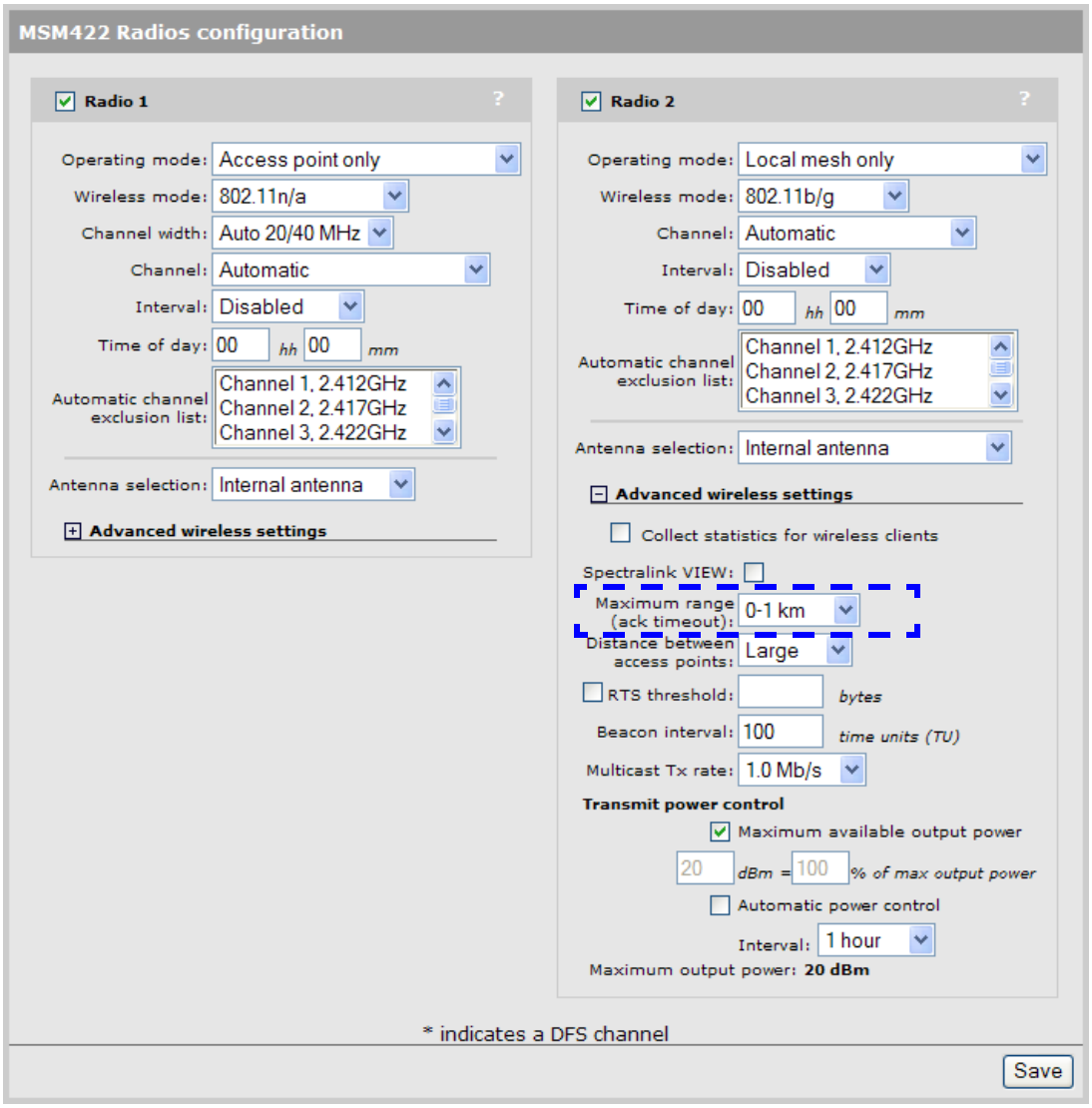
It is recommended that 802.11a is used for local mesh links whenever possible. This optimizes throughput and reduces the potential for interference because:

- Most Wi-Fi clients support 802.11b or b/g, therefore most APs are set to operate in the 2.4 GHz band. This frees the 5 GHz (802.11a) band for other applications such as local mesh.
- 802.11a provides more channels and more non-overlapping channels than 802.11b/g.
- Assuming an optimal implementation, 802.11a supports up to 54 Mbps for data throughput, providing a *fat pipe* for traffic exchange.
- Keep in mind that there are limitations inherent in using 802.11a, most notably shorter reach when compared to 2.4 GHz-based technology. Even so, 802.11a is a good choice in general.

Maximum range (ack timeout)

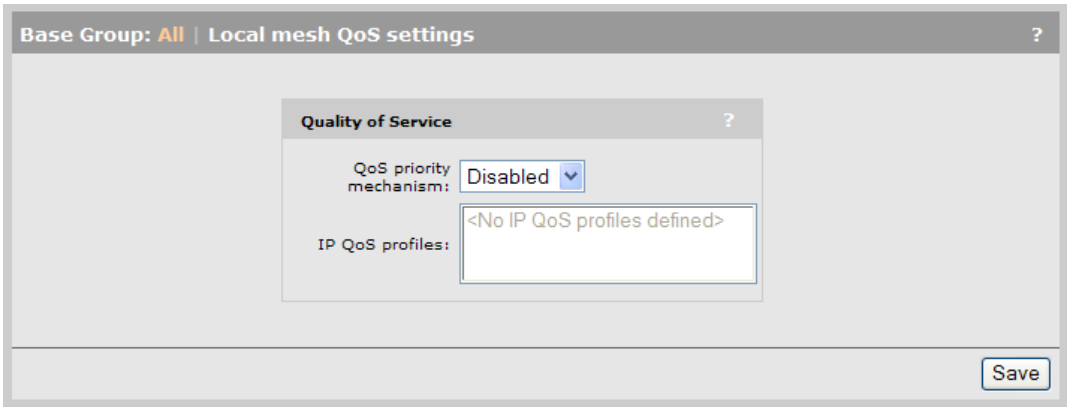
This is a global setting that is configurable on the **Radio** page when the **Operating mode** is set to **Local mesh**. It fine tunes internal timeout settings to account for the distance that a link spans. For normal operation, it is set to less than 1 km.

This is a global setting that applies to all wireless connections made with a radio, not just for local mesh links. Therefore, if you are also using a radio to access an AP, adjusting this setting may lower the performance for users with marginal signal strength or when interference is present. (Essentially, it means that if a frame needs to be retransmitted it will take longer before the actual retransmit takes place.)


MSM422 Radios configuration
Radio 1
Operating mode: Access point only
Wireless mode: 802.11n/a
Channel width: Auto 20/40 MHz
Channel: Automatic
Interval: Disabled
Time of day: 00 hh 00 mm
Automatic channel exclusion list: Channel 1, 2.412GHz Channel 2, 2.417GHz Channel 3, 2.422GHz
Antenna selection: Internal antenna
Advanced wireless settings
Radio 2
Operating mode: Local mesh only
Wireless mode: 802.11b/g
Channel: Automatic
Interval: Disabled
Time of day: 00 hh 00 mm
Automatic channel exclusion list: Channel 1, 2.412GHz Channel 2, 2.417GHz Channel 3, 2.422GHz
Antenna selection: Internal antenna
Advanced wireless settings
Collect statistics for wireless clients
Spectralink VIEW:
Maximum range (ack timeout): 0-1 km
Distance between access points: Large
RTS threshold: bytes
Beacon interval: 100 time units (TU)
Multicast Tx rate: 1.0 Mb/s
Transmit power control
Maximum available output power
20 dBm = 100 % of max output power
Automatic power control
Interval: 1 hour
Maximum output power: 20 dBm
* indicates a DFS channel
Save

Quality of service

The local mesh feature enables you to define a quality of service (QoS) setting that will govern how traffic is sent on all wireless links.



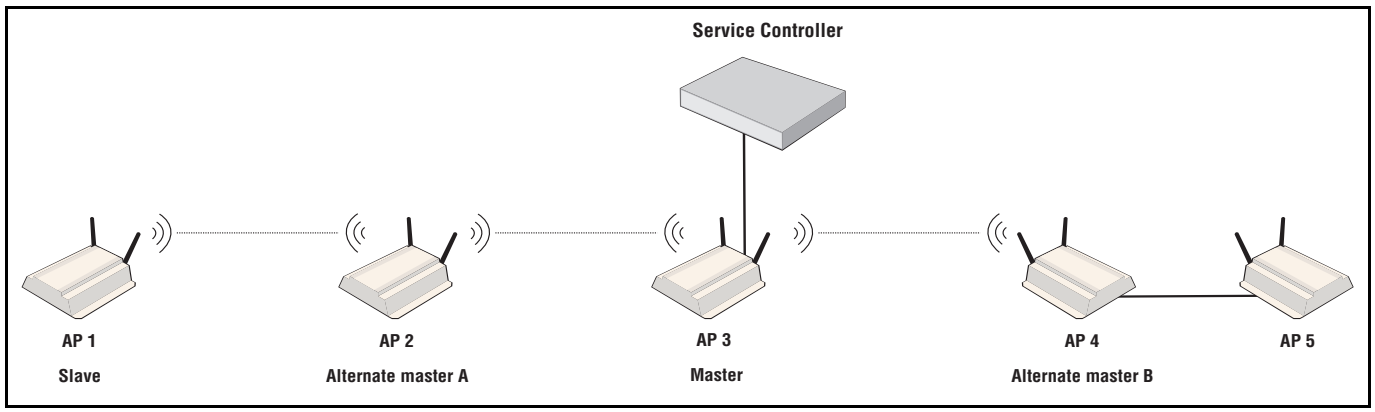
The QoS setting on all nodes in a local mesh must be the same.

Note

When traffic is forwarded onto a local mesh link from a VSC, the QoS settings on the VSC take priority. For example, if you define a VSC with a QoS setting of VSC-based High, then traffic from this VSC will traverse the local mesh on queue 2 even if the QoS setting on the local mesh is VSC-based Low (queue 4).

Provisioning local mesh links

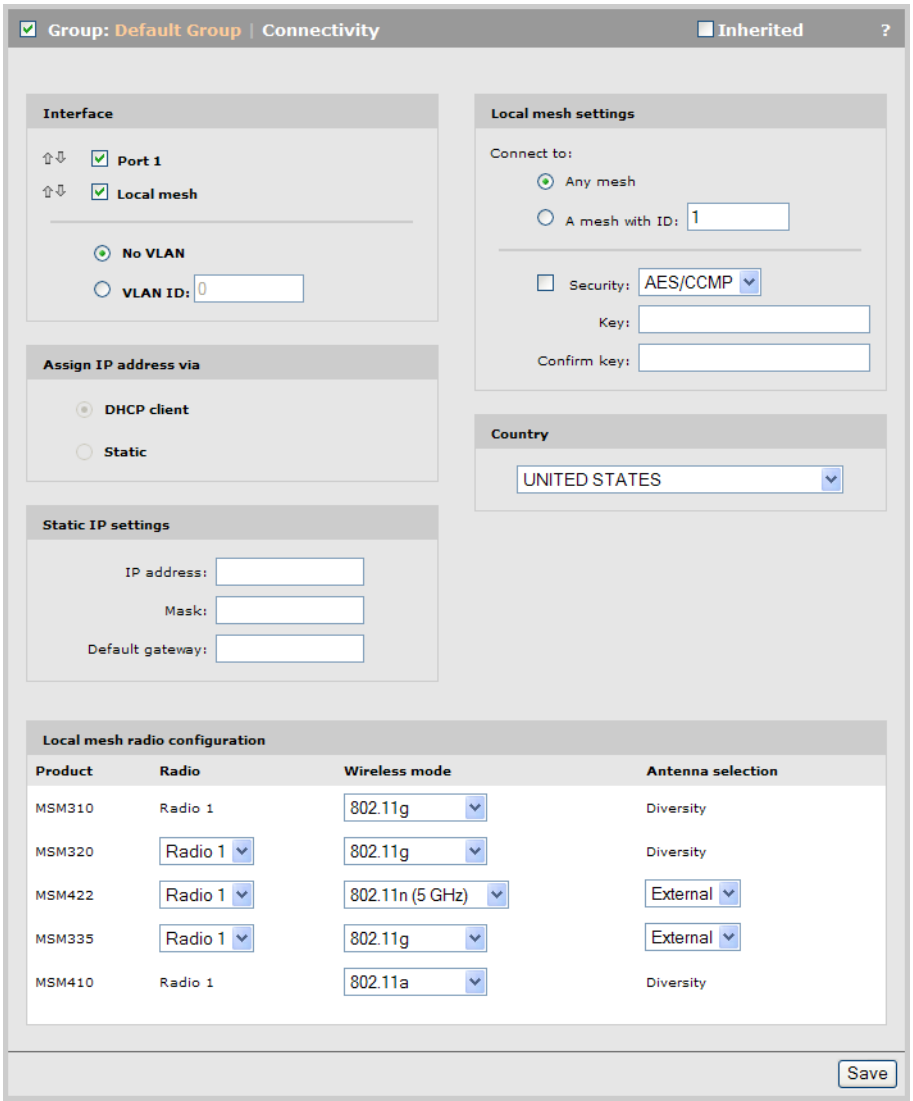
APs operating in controlled mode must be able to discover and connect with a service controller. When operating as part of a local mesh, *any AP that can **only** discover the service controller via a wireless link must be provisioned* before being deployed. In this example, AP 1, AP 2, and AP 4 must be provisioned prior to deployment for discovery to be successful. (Since AP is using a wired link, it does not need to be provisioned for this scenario.)



Provisioning is done before APs are deployed using either of the following methods:

- Directly connect to each AP and use its management tool to define provisioning settings.
- Connect the APs to the service controller (either directly via the LAN port or through a local area network). After the APs are discovered, use the service controller management tool to define provisioning settings by opening the **Provisioning > Connectivity** page at either the group or AP level.

In the this example, AP 1, AP 2, and AP 4 are all provisioned with the same settings as follows:



Use the Local mesh radio configuration table to define local mesh settings for each product type.

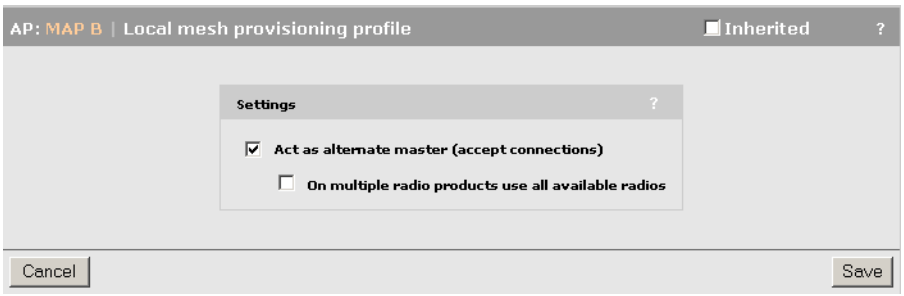
- **Product:** Indicates the product type.
- **Radio:** Select the radio that will be used for the local mesh.
- **Wireless mode:** Select the wireless mode that will be used for the local mesh.

- **Antenna selection:** Select the antenna(s) on which the radio transmits and receives.
  - **Internal:** The internal antenna is used to transmit and receive.
  - **External:** The external antenna is used to transmit and receive.

Note

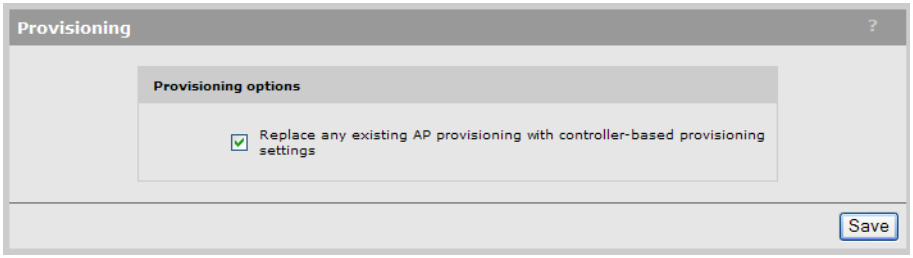
The service controller and all APs must all be configured for the same country, so that the local mesh established respects your local RF regulations. The service controller country setting is defined by selecting **Service Controller >> Management > Country**. APs with the wrong country setting will be displayed with a diagnostic of **Invalid Country** on the **Controlled APs >> Overview** page.

The local mesh provisioning profile for AP 2 needs to be set to alternate master mode so that it can support a connection from AP 1. Select AP 2 in the **Network Tree** and then open the **Configuration > Local mesh** page and select **Local mesh provisioning profile.**



Note

To enable the service controller to send provisioned settings to controlled APs, activate the **Enable provisioning of controlled APs** option on the **Service Controller >> Controlled APs > Provisioning** page.



Until this option is enabled, provisioned settings defined on the service controller are not sent to any controlled APs.

Once provisioning settings have been defined you need to update all controlled APs with the new settings by synchronizing them as described in *Synchronizing APs on page 3-22*.

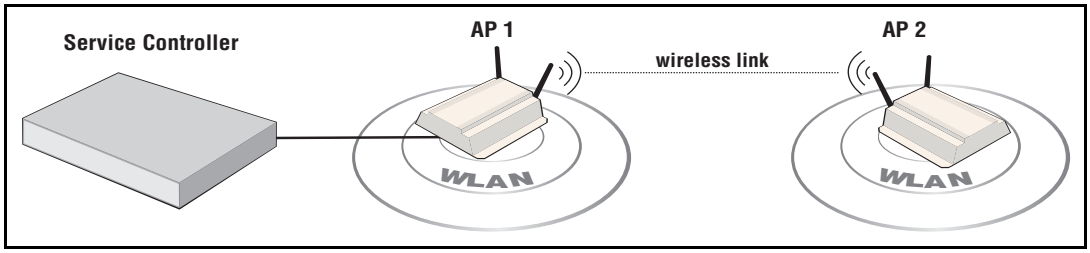
After an AP has been updated with provisioned settings, the provisioned settings do not become active until the AP is restarted, or a **Remove and rediscover** action is executed on the **Controlled APs >> Configured APs** page.

Sample local mesh deployments

RF extension

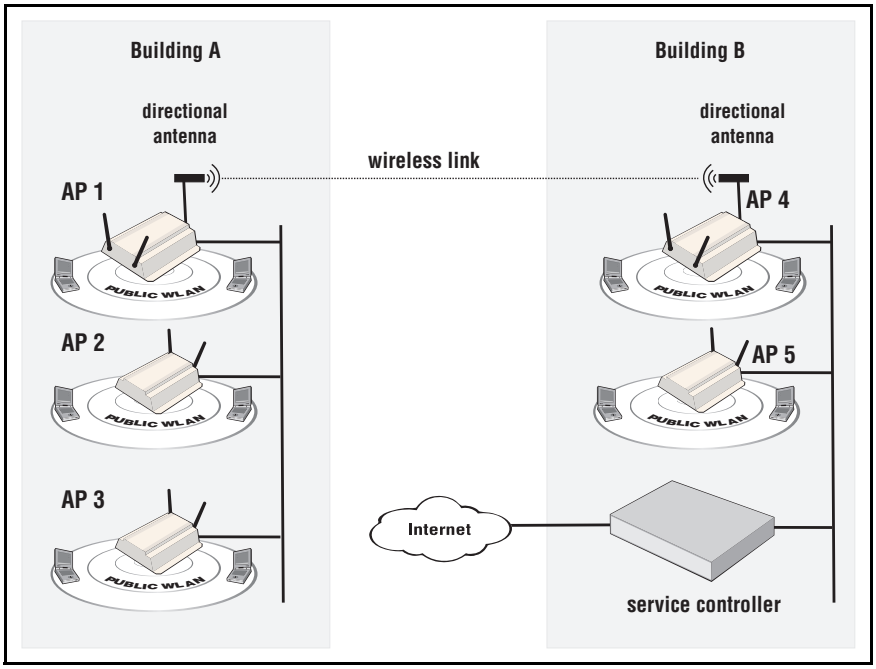
Local mesh provides an effective solution for extending wireless coverage in situations where it is impractical or expensive to run cabling to an AP.

In this scenario, a wireless bridge is used to extend coverage of the wireless network. Both APs are equipped with omni-directional antennas, enabling them to deliver both AP capabilities and wireless bridging using local mesh capabilities.



Building-to-building connection

You can also use local mesh to create point-to-point links over longer distances. in this scenario, two dual-radio APs create a wireless link between networks in two adjacent buildings. Each AP is equipped with a directional external antenna attached to radio 1 to provide the wireless link. Omnidirectional antennas are installed on radio 2 to provide AP capabilities. The two APs are placed within line of sight.



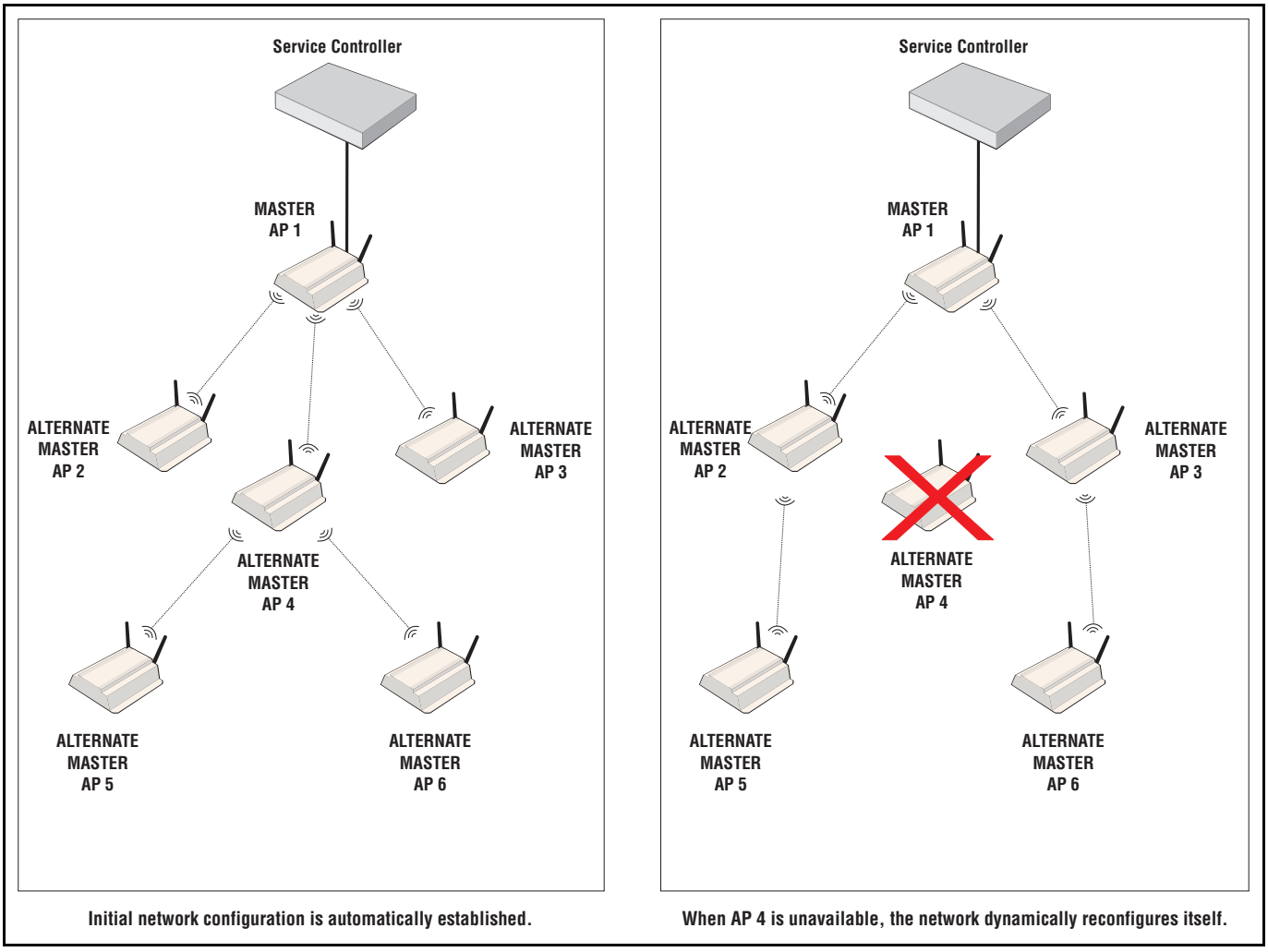
Note In the above example, all APs must connect to the backbone network via port 1.

Dynamic network

In this scenario, a service controller is deployed with several APs to provide wireless coverage of a large area. Instead of using a backbone LAN, wireless links are used to interconnect all APs.

AP 1 is the *master*. It provides the connection to the wired network and a wireless link to the other APs. The other APs automatically established their links to the master based on a balance between SNR (signal to noise ratio) and hops, to provide the most efficient network topology.

If a node becomes unavailable, the links dynamically adjust to find the optimum path to the master.


Service Controller
MASTER AP 1
ALTERNATE MASTER AP 2
ALTERNATE MASTER AP 3
ALTERNATE MASTER AP 4
ALTERNATE MASTER AP 5
ALTERNATE MASTER AP 6
Initial network configuration is automatically established.
Service Controller
MASTER AP 1
ALTERNATE MASTER AP 2
ALTERNATE MASTER AP 3
ALTERNATE MASTER AP 4
ALTERNATE MASTER AP 5
ALTERNATE MASTER AP 6
When AP 4 is unavailable, the network dynamically reconfigures itself.

14

Working with autonomous APs

Contents

Key concepts 14-2
- Autonomous AP detection 14-3
- Viewing autonomous AP information 14-3
- Switching a controlled AP to autonomous mode 14-4

Configuring autonomous APs 14-4
- VSC definitions 14-5

Working with third-party autonomous APs 14-6
- VSC selection 14-6

Key concepts

This chapter describes how to use the service controller in conjunction with autonomous APs.

Tip

Most of this chapter applies to working with autonomous MSM APs. For third-party autonomous APs, see *Working with third-party autonomous APs on page 14-6*.

APs can operate in either controlled mode or autonomous mode. In controlled mode, the service controller provides centralized management of APs. This is the preferred operation mode. See *Chapter 3: Working with controlled APs*.

However, in some other cases it is necessary to operate APs in autonomous mode, for example under the following circumstances:

- When an AP is used to create a static WDS (local mesh) link. Controlled mode does not support static local mesh links. It is strongly recommended that dynamic WDS (local mesh) links be used. They provide the same capabilities but with greater flexibility. Furthermore, local mesh is supported in controlled mode.
- An AP at software version 4.x or earlier is used. Controlled mode is available on APs at software version 5.x or higher. It is strongly recommended that service controllers and autonomous APs be updated to the same software version, and preferably 5.x or higher. Controlled APs are automatically updated to the service controller software version.

It is recommended that you operate most MSM APs in controlled mode, reserving autonomous mode only for APs that need features unique to autonomous mode. In autonomous mode, the following functionalities are not available: Centralized management, L3 mobility, and WPA2 Opportunistic key caching.

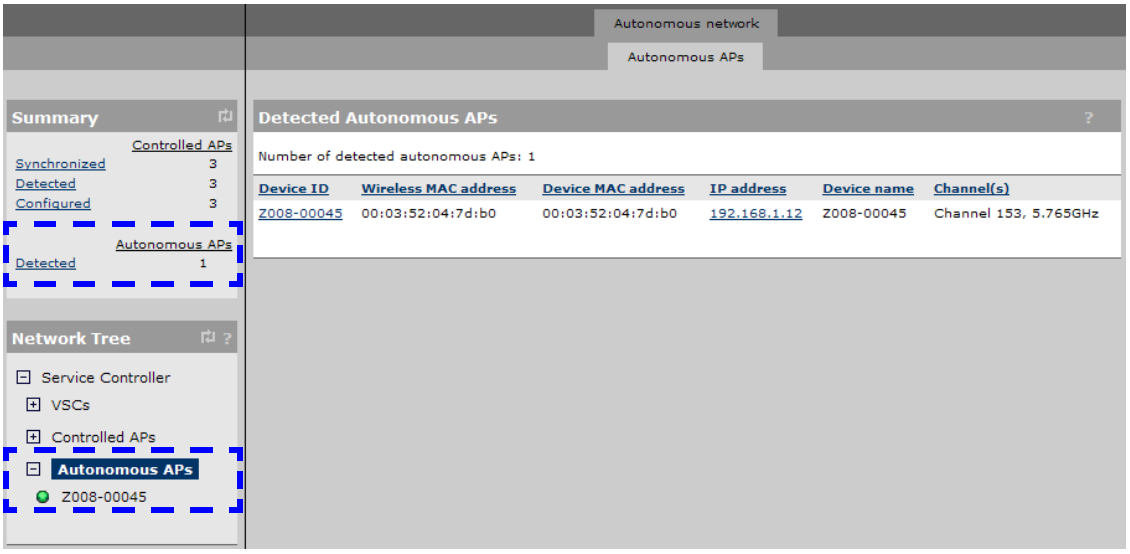
Autonomous AP detection

The service controller automatically detects all autonomous APs that have their CDP discovery option enabled (default setting) and are installed on the same subnet as the service controller.

To configure this CDP discovery, select **Network > CDP** on the AP management tool.

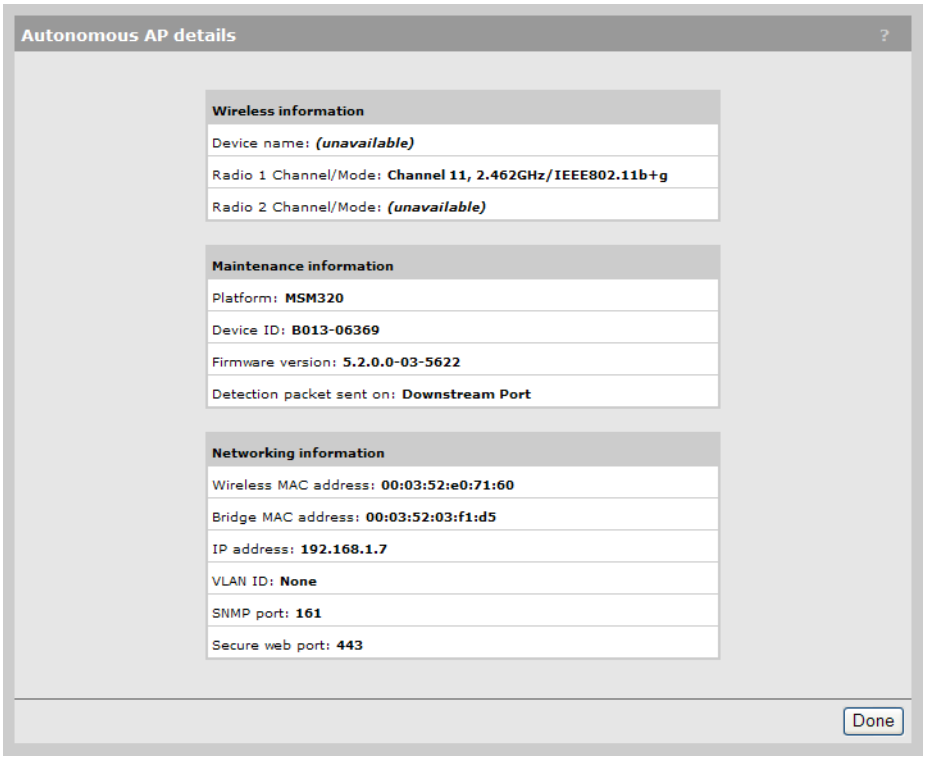
Viewing autonomous AP information

When the service controller detects at least one autonomous AP, the **Summary** box and the **Network Tree** are updated to include autonomous AP information as follows:



As shown in the above image, the **Summary** list includes a **Detected** link and count in the **Summary** list, and the **Network Tree** includes an **Autonomous APs** branch on **Service Controller**. These elements only appear when at least one autonomous APs has been detected. As shown, when Autonomous APs is selected, the list of **Detected Autonomous APs** list appears in the right pane.

Click a link in the **Device ID** column to display the **Autonomous APs details** like this:



You can also click the link in **IP address** column to launch the AP management tool. See the *MSM3xx/MSM4xx Management and Configuration Guide*.

Switching a controlled AP to autonomous mode

To switch a controlled AP to autonomous mode, select the AP in the **Default Group** branch of the Network Tree, and then in the right pane select **Maintenance > System** and select **Switch to Autonomous Mode**.

Note

The AP will restart and lose all configuration settings received from the service controller, returning to its default configuration. You can then configure it via its management tool.

Configuring autonomous APs

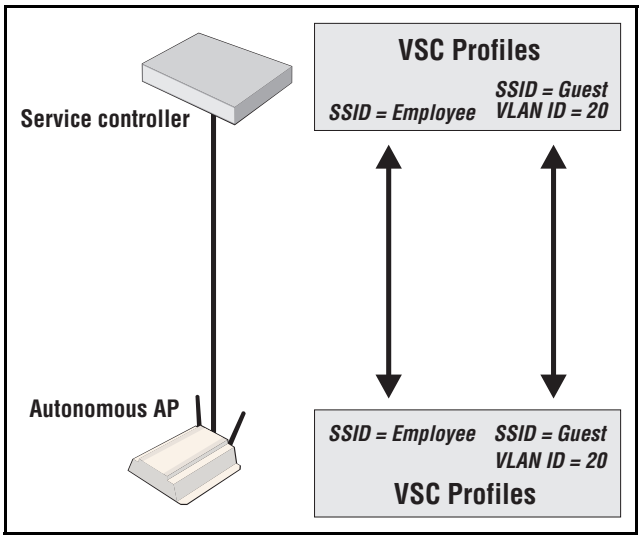
Autonomous APs must be configured via their own management tool. For convenience, you can launch an autonomous AP management tool from within the service controller management tool by clicking the link in the IP address column of the Detected Autonomous APs page, providing network access is possible.

When connecting one or more autonomous APs to co-exist with a service controller, some configuration issues must be addressed to ensure that data traffic and management traffic is able to flow between both devices.

If the management computer connects to the AP through the service controller Internet port but the AP connects via the LAN port, static NAT mappings will be needed to be created to allow traffic to go through the service controller firewall. See the *MSM3xx/MSM4xx Management and Configuration Guide*.

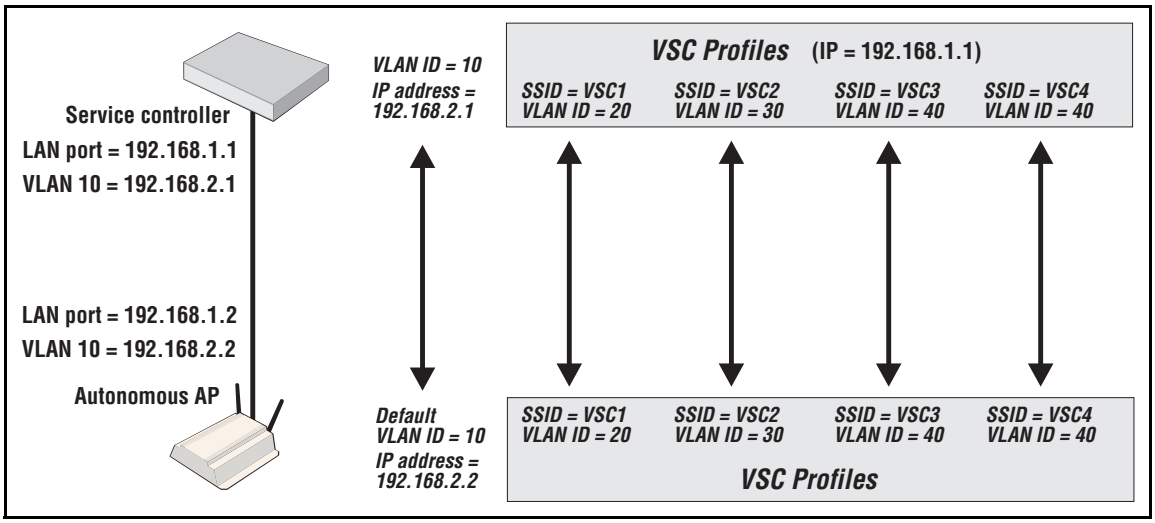
VSC definitions

Although the service controller cannot configure autonomous APs, the APs can work with the service controller to benefit from the advanced access control services a service controller provides. To do this, use the autonomous AP management tool to configure VSCs that use the same SSID and/or VLAN as already configured on the service controller. The matching VSC configuration is illustrated as follows:



Management with VLANs

When operating in a VLAN environment, management traffic can be carried on its own VLAN. Configure the VSC on both the autonomous AP and the service controller as illustrated here:



In this example, the traffic for each wireless network is carried on its own VLAN. This leaves only management traffic from the autonomous AP on VLAN 10 segment. A static IP is assigned on both ends to permit the two devices to communicate.

Working with third-party autonomous APs

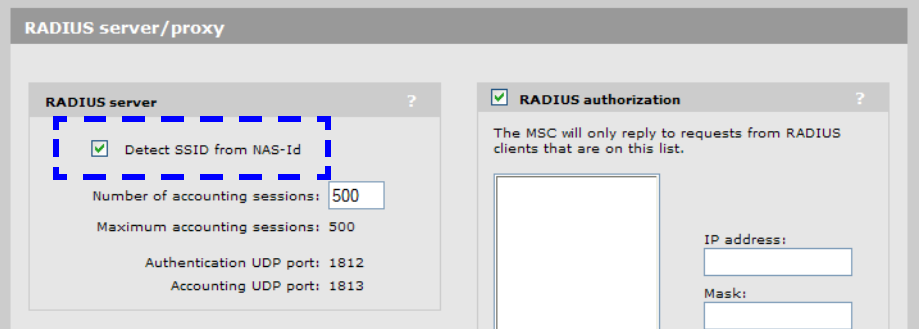
Third-party APs can be used with a service controller with both access controlled and non-access controlled VSCs.

VSC selection

User traffic from third-party APs is mapped to a VSC on the service controller in the same way as for MSM APs. See *Using multiple VSCs on page 2-24*. This means that traffic is assigned to the default VSC, unless it is on a VLAN, in which case it is assigned to the VSC with matching VLAN ingress definition.

Because the HP ProCurve Networking location-aware feature is not available on third-party APs, support for VSC selection using an SSID requires that the following additional configuration be performed:

- Configure the AP to send its SSID as the NAS ID in all **authentication and accounting** requests.
- Enable the **Detect SSID from NAS-Id** option on the **Service controller >> Authentication > RADIUS server** page.


RADIUS server/proxy
RADIUS server
Detect SSID from NAS-Id
Number of accounting sessions: 500
Maximum accounting sessions: 500
Authentication UDP port: 1812
Accounting UDP port: 1813
RADIUS authorization
The MSC will only reply to requests from RADIUS clients that are on this list.
IP address:
Mask:

15

Maintenance

Contents

Config file management 15-2
- Manual configuration file management 15-2
- Scheduled operations 15-3

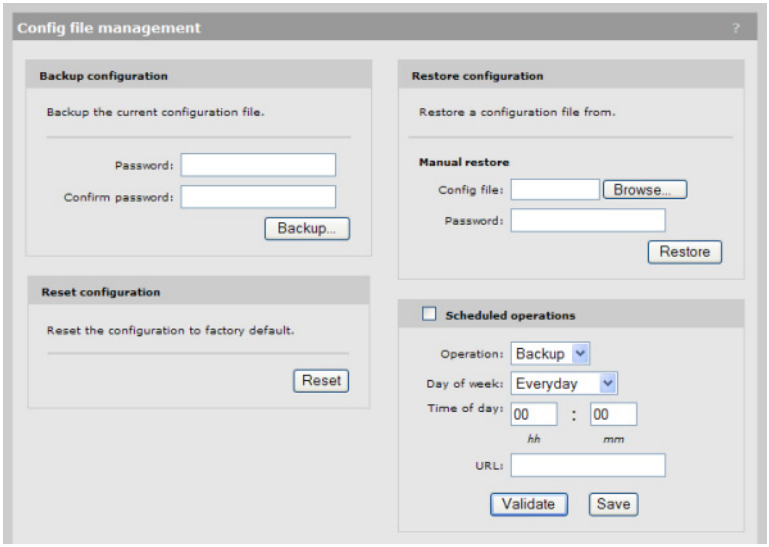
Software updates 15-5
- Performing an immediate software update 15-5
- Performing a scheduled software update 15-6

Managing licenses 15-7
- Factory installed licenses 15-7
- User installed licenses 15-7
- License management 15-8
- Factory reset considerations 15-8

Config file management

The configuration file contains all the settings that customize the operation of the service controller. You can save and restore the configuration file manually or automatically.

Select **Maintenance > Config file management**.



Manual configuration file management

The following options are available for manual configuration file management.

Backup configuration

The **Backup configuration** group box enables you to back up your configuration settings so that they can be easily restored in case of failure. You can also use this option if you want to directly edit the configuration file.

Before you install new software, you should always back up your current configuration. Select **Backup** to start the process. You are prompted for the location in which to save the configuration file.

If you specify a **Password,** the configuration file is protected by encrypting sensitive fields (example, passwords, secrets, and certificates) with a key based on the password. See also *Restore configuration on page 15-3*.

Note

Even without a password, the certificates are still encrypted but with a key that is identical on all devices.

Note

The local username and password for the administrative users are not saved to the backup configuration file. If you upload a configuration file, the current username and password are not overwritten.

Note Local user accounts are backed up but are not encrypted.

Reset configuration

See *Appendix C: Resetting to factory defaults*.

Restore configuration

The **Restore configuration** group box enables you to reload a previously saved backup configuration file.

This feature enables you to maintain several configuration files with different settings, which can be useful if you must frequently alter the configuration of the service controller or if you are managing several service controllers from a central site.

Use the following steps to restore a saved configuration file.

1. Select **Maintenance > Config file management.** The **Config file management** page opens.
2. In the **Restore configuration** group box under **Manual restore,** select **Browse** to navigate to and select the configuration file that you want to restore.
3. If the configuration file is protected with a password (see *Backup configuration on page 15-2*) you must supply the correct password to restore the complete configuration. If you supply an invalid password, all settings are restored except the certificates.
4. To upload the selected file to the service controller, select **Restore.**

Note The service controller automatically restarts when the upload is complete.

Scheduled operations

The **Scheduled operations** group box enables you to schedule unattended backups or restorations of the service controller configuration file. See also *Performing a scheduled software update on page 15-6*.

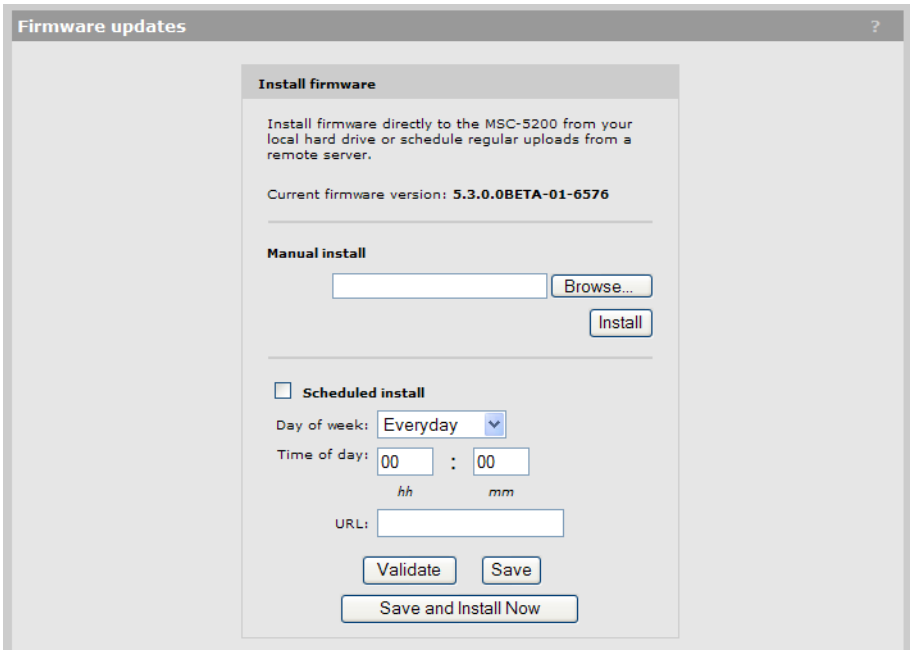
Use the following steps to schedule a backup or restoration of the service controller configuration file.

1. Select **Maintenance > Config file management.** The **Config file management** page opens.
2. At lower right, select the **Scheduled operations** checkbox.
3. Under **Operation,** select **Backup** or **Restore**.
4. Under **Day of week,** select **Everyday,** or select a specific day of the week on which to perform the backup or restoration.

5. Under **Time of day,** specify the hour and minute on which to perform the backup or restoration. Use the format *hh mm*, where:
   - *hh* ranges from 00 to 23
   - *mm* ranges from 00 to 59.
6. Under **URL,** specify the path that leads to the remote directory in which to save the configuration file or from which to load the configuration file. For example:
   - **ftp://username:password@192.168.132.11/new.cfg**
   - **http://192.168.132.11/new.cfg**
7. To confirm that the specified **URL** is correct, select **Validate.**
8. To commit the schedule that you have configured, select **Save.**

Software updates

Service controller software updates are managed by selecting **Maintenance > Firmware updates.**



Caution

- Before updating be sure to check for update issues in the Release Notes.
- Even though configuration settings are preserved during software updates, it is recommended that you backup your configuration settings before updating.
- After updating the service controller software, controlled APs are automatically updated to the same version that is installed on the service controller. At the end of the update process, the service controller and all controlled APs automatically restart, causing all users to be disconnected. Once the service controller and APs resume operation, all users must reconnect. To minimize network disruption, use the scheduled install option to have updates performed outside of peak usage hours.

Performing an immediate software update

To update the service controller software now, **Browse** to the software file (extension .cim) and then select **Install.**

Performing a scheduled software update

The service controller can automatically retrieve and install software from a remote Web site identified by its URL.

To schedule software installation, follow this procedure:

1. Enable **Scheduled install**.
2. For **Day of week** select a specific day or **Everyday** and set **Time of day**.
3. For **URL**, specify an ftp or http address like this:
   - **ftp://username:password@192.168.132.11/newsoftware.cim**
   - **http://192.168.132.11/newsoftware.cim**
4. **Validate** the URL.
5. To commit the schedule, select **Save.**
6. Or, to commit the schedule and also update the software immediately, select **Save and Install Now**.

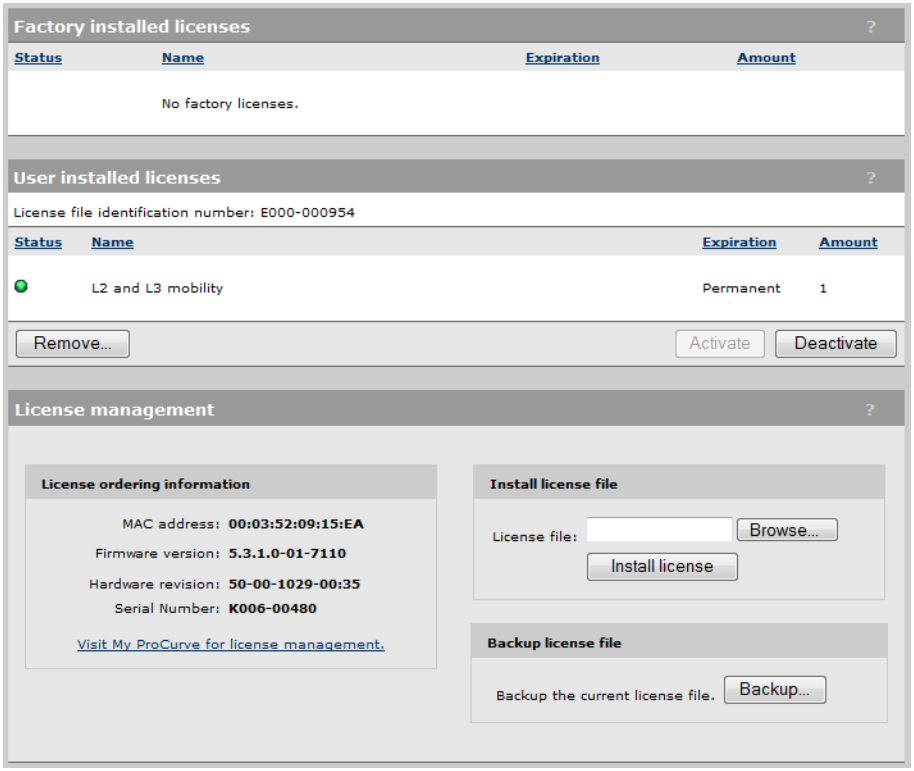
Note

Before a scheduled software update is performed, only the first few bytes of the software file are downloaded to determine if the software is newer than the current. If it is not, the download stops and the software is not updated at this time. Which means that if by accident you try to upload the same software, it will not affect the operation of your network.

Managing licenses

Some service controller features are optional, becoming activated only when a license is installed. Licenses can be installed at the factory or by the user.

To view and manage licenses, select **Service Controller >> Maintenance > Licenses**.



Factory installed licenses

This table lists all licenses installed on the service controller at the factory. These licenses are always active and cannot be removed or disabled.

If you purchase a license when you order your service controller, the license is factory-installed.

User installed licenses

This table lists all user installed licenses. Work with these licenses as follows:

- Select **Deactivate** to temporarily deactivate all user installed licenses. Any features that depend on these licenses will become unavailable.
- Select **Activate** to activate user-installed licenses that have been deactivated.
- Select **Remove** to delete all user installed licenses. Before removing licenses, be sure to first backup the license file to your hard drive, using the **Backup** button.

License management

- To order a new feature license, take note of the **License ordering information** and then select **Visit My ProCurve for license management**.
- To install a license file, **Browse** to the file and then select **Install License**.
- Select **Backup** to save all user-defined licenses in a single file.

Factory reset considerations

After a service controller has been reset to its factory defaults, factory-installed licenses are automatically re-activated but user-installed licenses remain in a deactivated state until manually activated. This is done to ensure a true factory-default reset.

A

Safety and EMC regulatory statements

Contents

Safety Information A-2

Informations concernant la sécurité A-2

Hinweise zur Sicherheit A-3

Considerazioni sulla sicurezza A-4

Consideraciones sobre seguridad A-5

Safety Information (Japan) A-6

Safety Information (China) A-7

EMC Regulatory Statements A-8

- U.S.A. A-8
- Japan A-8

Recycle Statements A-10

- Waste Electrical and Electronic Equipment (WEEE) Statements A-10

Safety Information

Documentation reference symbol. If the product is marked with this symbol, see the product documentation to get more information about the product.

WARNING A **WARNING** in the manual denotes a hazard that can cause injury or death.

Caution A Caution in the manual denotes a hazard that can damage equipment.

Do not proceed beyond a **WARNING** or Caution notice until you have understood the hazardous conditions and have taken appropriate steps.

Grounding
These are safety class I products and have protective earthing terminals. There must be an uninterruptible safety earth ground from the main power source to the product's input wiring terminals, power cord, or supplied power cord set. Whenever it is likely that the protection has been impaired, disconnect the power cord until the ground has been restored.

For LAN cable grounding

- If your LAN covers an area served by more than one power distribution system, be sure their safety grounds are securely interconnected.
- LAN cables may occasionally be subject to hazardous transient voltages (such as lightning or disturbances in the electrical utilities power grid). Handle exposed metal components of the network with caution.

Servicing
There are no user-serviceable parts inside these products. Any servicing, adjustment, maintenance, or repair must be performed only by service-trained personnel.

These products do not have a power switch; they are powered on when the power cord is plugged in.

Informations concernant la sécurité

Symbole de référence à la documentation. Si le produit est marqué de ce symbole, reportez-vous à la documentation du produit afin d'obtenir des informations plus détaillées.

WARNING Dans la documentation, un**WARNING** indique un danger susceptible d'entraîner des dommages corporels ou la mort.

Caution Un texte de mise en garde intituléCaution indique un danger susceptible de causer des dommages à l'équipement.

Ne continuez pas au-delà d'une rubrique **WARNING** ou Caution avant d'avoir bien compris les conditions présentant un danger et pris les mesures appropriées.

Cet appareil est un produit de classe I et possède une borne de mise à la terre. La source d'alimentation principale doit être munie d'une prise de terre de sécurité installée aux bornes du câblage d'entrée, sur le cordon d'alimentation ou le cordon de raccordement fourni avec le produit. Lorsque cette protection semble avoir été endommagée, débrancher le cordon d'alimentation jusqu'à ce que la mise à la terre ait été réparée.

Mise à la terre du câble de réseau local:

- si votre réseau local s'étend sur une zone desservie par plus d'un système de distribution de puissance, assurez-vous que les prises de terre de sécurité soient convenablement interconnectées.
- Les câbles de réseaux locaux peuvent occasionnellement être soumis à des surtensions transitoires dangereuses (telles que la foudre ou des perturbations dans le réseau d'alimentation public). Manipulez les composants métalliques du réseau avec précautions.

Aucune pièce contenue à l'intérieur de ce produit ne peut être réparée par l'utilisateur. Tout dépannage, réglage, entretien ou réparation devra être confié exclusivement à un personnel qualifié.

Cet appareil ne comporte pas de commutateur principal ; la mise sous tension est effectuée par branchement du cordon d'alimentation.

Hinweise zur Sicherheit

Symbol für Dokumentationsverweis. Wenn das Produkt mit diesem Symbol markiert ist, schlagen Sie bitte in der Produktdokumentation nach, um mehr Informationen über das Produkt zu erhalten.

WARNING Eine**WARNING** in der Dokumentation symbolisiert eine Gefahr, die Verletzungen oder sogar Todesfälle verursachen kann.

Caution Caution in der Dokumentation symbolisiert eine Gefahr, die dis Gerät beschädigen kann.

Fahren Sie nach dem Hinweis **WARNING** oder Caution erst fort, nachdem Sie den Gefahrenzustand verstanden und die entsprechenden Maßnahmen ergriffen haben.

Dies ist ein Gerät der Sicherheitsklasse I und verfügt über einen schützenden Erdungsterminal. Der Betrieb des Geräts erfordert eine ununterbrochene Sicherheitserdung von der Hauptstromquelle zu den Geräteingabeterminals, den Netzkabeln oder dem mit Strom belieferten Netzkabelsatz voraus. Sobald Grund zur Annahme besteht, daß der Schutz beeinträchtigt worden ist, das Netzkabel aus der Wandsteckdose herausziehen, bis die Erdung wiederhergestellt ist.

Für LAN-Kabelerdung:

- Wenn Ihr LAN ein Gebiet umfaßt, das von mehr als einem Stromverteilungssystem beliefert wird, müssen Sie sich vergewissern, daß die Sicherheitserdungen fest untereinander verbunden sind.
- LAN-Kabel können gelegentlich gefährlichen Übergangsspannungen ausgesetzt werden (beispielsweise durch Blitz oder Störungen in dem Starkstromnetz des Elektrizitätswerks). Bei der Handhabung exponierter Metallbestandteile des Netzwerkes Vorsicht walten lassen.

Dieses Gerät enthält innen keine durch den Benutzer zu wartenden Teile. Wartungs-, Anpassungs-, Instandhaltungs- oder Reparaturarbeiten dürfen nur von geschultem Bedienungspersonal durchgeführt werden.

Dieses Gerät hat keinen Netzschalter; es wird beim Anschließen des Netzkabels eingeschaltet.

Considerazioni sulla sicurezza

Simbolo di riferimento alla documentazione. Se il prodotto è contrassegnato da questo simbolo, fare riferimento alla documentazione sul prodotto per ulteriori informazioni su di esso.

WARNING — La dicitura **WARNING**denota un pericolo che può causare lesioni o morte.

Caution — La dicituraCaution denota un pericolo che può danneggiare le attrezzature.

Non procedere oltre un avviso di **WARNING** o di Cautionprima di aver compreso le condizioni di rischio e aver provveduto alle misure del caso.

Questo prodotto è omologato nella classe di sicurezza I ed ha un terminale protettivo di collegamento a terra. Dev'essere installato un collegamento a terra di sicurezza, non interrompibile che vada dalla fonte d'alimentazione principale ai terminali d'entrata, al cavo d'alimentazione oppure al set cavo d'alimentazione fornito con il prodotto. Ogniqualvolta vi sia probabilità di danneggiamento della protezione, disinserite il cavo d'alimentazione fino a quando il collegaento a terra non sia stato ripristinato.

Per la messa a terra dei cavi LAN:

- se la vostra LAN copre un'area servita da più di un sistema di distribuzione elettrica, accertatevi che i collegamenti a terra di sicurezza siano ben collegati fra loro;
- i cavi LAN possono occasionalmente andare soggetti a pericolose tensioni transitorie (ad esempio, provocate da lampi o disturbi nella griglia d'alimentazione della società elettrica); siate cauti nel toccare parti esposte in metallo della rete.

Nessun componente di questo prodotto può essere riparato dall'utente. Qualsiasi lavoro di riparazione, messa a punto, manutenzione o assistenza va effettuato esclusivamente da personale specializzato.

Questo apparato non possiede un commutatore principale; si mette scotto tensione all'inserirsi il cavo d'alimentazione.

Consideraciones sobre seguridad

Símbolo de referencia a la documentación. Si el producto va marcado con este símbolo, consultar la documentación del producto a fin de obtener mayor información sobre el producto.

WARNING — Una**WARNING** en la documentación señala un riesgo que podría resultar en lesiones o la muerte.

Caution — Una Caution en la documentación señala un riesgo que podría resultar en averías al equipo.

No proseguir después de un símbolo de **WARNING** o Caution hasta no haber entendido las condiciones peligrosas y haber tomado las medidas apropiadas.

Este aparato se enmarca dentro de la clase I de seguridad y se encuentra protegido por una borna de puesta a tierra. Es preciso que exista una puesta a tierra continua desde la toma de alimentación eléctrica hasta las bornas de los cables de entrada del aparato, el cable de alimentación o el juego de cable de alimentación suministrado. Si existe la probabilidad de que la protección a tierra haya sufrido desperfectos, desenchufar el cable de alimentación hasta haberse subsanado el problema.

Puesta a tierra del cable de la red local (LAN):

- Si la LAN abarca un área cuyo suministro eléctrico proviene de más de una red de distribución de electricidad, cerciorarse de que las puestas a tierra estén conectadas entre sí de modo seguro.
- Es posible que los cables de la LAN se vean sometidos de vez en cuando a voltajes momentáneos que entrañen peligro (rayos o alteraciones en la red de energía eléctrica). Manejar con precaución los componentes de metal de la LAN que estén al descubierto.

Este aparato no contiene pieza alguna susceptible de reparación por parte del usuario. Todas las reparaciones, ajustes o servicio de mantenimiento debe realizarlos solamente el técnico.

Este producto no tiene interruptor de potencia; se activa cuando se enchufa el cable de alimentación.

Safety Information (Japan)

安全性の考慮

安全記号

マニュアル参照記号。製品にこの記号がついている場合はマニュアルを参照し、注意事項等をご確認ください。

WARNING　マニュアル中の「WARNING」は人身事故の原因となる危険を示します。

CAUTION　マニュアル中の「CAUTION」は装置破損の原因となる危険を示します。

「WARNING」や「CAUTION」の項は飛ばさないで必ずお読みください。危険性に関する記載事項をよく読み、正しい手順に従った上で次の事項に進んでください。

これは安全性クラスIの製品で保護用接地端子を備えています。主電源から製品の入力配線端子、電源コード、または添付の電源コード・セットまでの間、切れ目のない安全接地が存在することが必要です。もしこの保護回路が損なわれたことが推測されるときは、接地が修復されるまで電源コードを外しておいてください。

LAN ケーブルの接地に関して:

- もし貴社のLANが複数の配電システムにより電力を受けている領域をカバーしている場合には、それらのシステムの安全接地が確実に相互に結合されていることを確認してください。
- LAN ケーブルは時として危険な過度電圧（例えば雷や、配電設備の電力網での障害）にさらされることがあります。露出した金属部分の取扱いには十分な注意をはらってください。

本製品の内部にはユーザーが修理できる部品はありません。サービス、調整、保守および修理はサービス訓練を受けた専門家におまかせください。

本製品には電源スイッチがありません。電源コードを接続したとき電源入となります。

Japan Power Cord Warning

製品には、同梱された電源コードをお使い下さい。
同梱された電源コードは、他の製品では使用出来ません。

Safety Information (China)

HP网络产品使用安全手册

使用须知

欢迎使用惠普网络产品，为了您及仪器的安全，请您务必注意如下事项:

1. 仪器要和地线相接，要使用有正确接地插头的电源线，使用中国国家规定 的220V 电源。
2. 避免高温和尘土多的地方，否则易引起仪器内部部件的损坏。
3. 避免接近高温，避免接近直接热源，如直射太阳光、暖气等其它发热体。
4. 不要有异物或液体落入机内，以免部件短路。
5. 不要将磁体放置于仪器附近。

警告

为防止火灾或触电事故，请不要将该机放置于淋雨或潮湿处。

安装

安装辅助管理模块，请参看安装指南。

保修及技术支持

如果您按照以上步骤操作时遇到了困难，或想了解其它产品性能，请按以下 方式与我们联络。

如是硬件故障:

1. 与售出单位或当地维修机构联系。
2. 中国惠普有限公司维修中心地址:
   北京市海淀区知春路49号 希格玛大厦
   联系电话: 010-62623888 转 6101
   邮政编码: 100080

如是软件问题:

1. 惠普用户响应中心热线电话: 010-65645959
2. 传真自动回复系统: 010-65645735

EMC Regulatory Statements

U.S.A.

FCC Class A (Applies to the MSM730/MSM750)
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. Operation of this equipment in a residential area may cause interference in which case the user will be required to correct the interference at his own expense.

FCC Class B (Applies to the MSM710)
This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. Theses limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and the receiver
- Connect the equipment into an outlet that is on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help."

CAUTION Any changes or modifications to this equipment not expressly approved by the

Hewlett-Packard Company may cause harmful interference and void the FCC authorization to operate this equipment."

Japan

VCCI Class A (Applies to the MSM730/MSM750)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI Class B (Applies to the MSM710)

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。
取り扱い説明書に従って正しい取り扱いをして下さい。

Korea

Class A (Applies to the MSM730/MSM750)

사용자 안내문 : A 급기기

이기기는 업무용으로 전자파 적합등록을 받은 기기이오니, 판매자 또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 구입하셨을 때에는 구입한 곳에서 비업무용으로 교환하시기 바랍니다.

Class B (Applies to the MSM710)

B급 기기 (가정용 방송통신기기)	이 기기는 가정용(B급)으로 전자파적합등록을 한 기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다.

Taiwan

Class A (Applies to the MSM730/MSM750)

警告使用者：這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Recycle Statements

Waste Electrical and Electronic Equipment (WEEE) Statements

Disposal of Waste Equipment by Users in Private Household in the European Union

This symbol on the product or on its packaging indicates that this product must not be disposed of with your other household waste. Instead, it is your responsibility to dispose of your waste equipment by handing it over to a designated collection point for the recycling of waste electrical and electronic equipment. The separate collection and recycling of your waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Likvidace zařízení soukromými domácími uživateli v Evropské unii

Tento symbol na produktu nebo balení označuje výrobek, který nesmí být vyhozen spolu s ostatním domácím odpadem. Povinností uživatele je předat takto označený odpad na předem určené sběrné místo pro recyklaci elektrických a elektronických zařízení. Okamžité třídění a recyklace odpadu pomůže uchovat přírodní prostředí a zajistí takový způsob recyklace, který ochrání zdraví a životní prostředí člověka. Další informace o možnostech odevzdání odpadu k recyklaci získáte na příslušném obecním nebo městském úřadě, od firmy zabývající se sběrem a svozem odpadu nebo v obchodě, kde jste produkt zakoupili.

Bortskaffelse af affald fra husstande i den Europæiske Union

Hvis produktet eller dets emballage er forsynet med dette symbol, angiver det, at produktet ikke må bortskaffes med andet almindeligt husholdningsaffald. I stedet er det dit ansvar at bortskaffe kasseret udstyr ved at aflevere det på den kommunale genbrugsstation, der forestår genvinding af kasseret elektrisk og elektronisk udstyr. Den centrale modtagelse og genvinding af kasseret udstyr i forbindelse med bortskaffelsen bidrager til bevarelse af naturlige ressourcer og sikrer, at udstyret genvindes på en måde, der beskytter både mennesker og miljø. Yderligere oplysninger om, hvor du kan aflevere kasseret udstyr til genvinding, kan du få hos kommunen, den lokale genbrugsstation eller i den butik, hvor du købte produktet.

Seadmete jäätmete kõrvaldamine eramajapidamistes Euroopa Liidus

See tootel või selle pakendil olev sümbol näitab, et kõnealust toodet ei tohi koos teiste majapidamisjäätmetega kõrvaldada. Teie kohus on oma seadmete jäätmed kõrvaldada, viies need elektri- ja elektroonikaseadmete jäätmete ringlussevõtmiseks selleks ettenähtud kogumispunkti. Seadmete jäätmete eraldi kogumine ja ringlussevõtmine kõrvaldamise ajal aitab kaitsta loodusvarasid ning tagada, et ringlussevõtmine toimub viisil, mis kaitseb inimeste tervist ning keskkonda. Lisateabe saamiseks selle kohta, kuhu oma seadmete jäätmed ringlussevõtmiseks viia, võtke palun ühendust oma kohaliku linnakantselei, majapidamisjäätmete kõrvaldamise teenistuse või kauplusega, kust Te toote ostsite.

Laitteiden hävittäminen kotitalouksissa Euroopan unionin alueella

Jos tuotteessa tai sen pakkauksessa on tämä merkki, tuotetta ei saa hävittää kotitalousjätteiden mukana. Tällöin hävitettävä laite on toimitettava sähkölaitteiden ja elektronisten laitteiden kierrätyspisteeseen. Hävitettävien laitteiden erillinen käsittely ja kierrätys auttavat säästämään luonnonvaroja ja varmistamaan, että laite kierrätetään tavalla, joka estää terveyshaitat ja suojelee luontoa. Lisätietoja paikoista, joihin hävitettävät laitteet voi toimittaa kierrätettäväksi, saa ottamalla yhteyttä jätehuoltoon tai liikkeeseen, josta tuote on ostettu.

Élimination des appareils mis au rebut par les ménages dans l'Union européenne

Le symbole apposé sur ce produit ou sur son emballage indique que ce produit ne doit pas être jeté avec les déchets ménagers ordinaires. Il est de votre responsabilité de mettre au rebut vos appareils en les déposant dans les centres de collecte publique désignés pour le recyclage des équipements électriques et électroniques. La collecte et le recyclage de vos appareils mis au rebut indépendamment du reste des déchets contribue à la préservation des ressources naturelles et garantit que ces appareils seront recyclés dans le respect de la santé humaine et de l'environnement. Pour obtenir plus d'informations sur les centres de collecte et de recyclage des appareils mis au rebut, veuillez contacter les autorités locales de votre région, les services de collecte des ordures ménagères ou le magasin dans lequel vous avez acheté ce produit.

Entsorgung von Altgeräten aus privaten Haushalten in der EU

Das Symbol auf dem Produkt oder seiner Verpackung weist darauf hin, dass das Produkt nicht über den normalen Hausmüll entsorgt werden darf. Benutzer sind verpflichtet, die Altgeräte an einer Rücknahmestelle für Elektro- und Elektronik-Altgeräte abzugeben. Die getrennte Sammlung und ordnungsgemäße Entsorgung Ihrer Altgeräte trägt zur Erhaltung der natürlichen Ressourcen bei und garantiert eine Wiederverwertung, die die Gesundheit des Menschen und die Umwelt schützt. Informationen dazu, wo Sie Rücknahmestellen für Ihre Altgeräte finden, erhalten Sie bei Ihrer Stadtverwaltung, den örtlichen Müllentsorgungsbetrieben oder im Geschäft, in dem Sie das Gerät erworben haben

Απόρριψη άχρηστου εξοπλισμού από χρήστες σε ιδιωτικά νοικοκυριά στην Ευρωπαϊκή Ένωση

Το σύμβολο αυτό στο προϊόν ή τη συσκευασία του υποδεικνύει ότι το συγκεκριμένο προϊόν δεν πρέπει να διατίθεται μαζί με τα άλλα οικιακά σας απορρίμματα. Αντίθετα, είναι δική σας ευθύνη να απορρίψετε τον άχρηστο εξοπλισμό σας παραδίδοντάς τον σε καθορισμένο σημείο συλλογής για την ανακύκλωση άχρηστου ηλεκτρικού και ηλεκτρονικού εξοπλισμού. Η ξεχωριστή συλλογή και ανακύκλωση του άχρηστου εξοπλισμού σας κατά την απόρριψη θα συμβάλει στη διατήρηση των φυσικών πόρων και θα διασφαλίσει ότι η ανακύκλωση γίνεται με τρόπο που προστατεύει την ανθρώπινη υγεία και το περιβάλλον. Για περισσότερες πληροφορίες σχετικά με το πού μπορείτε να παραδώσετε τον άχρηστο εξοπλισμό σας για ανακύκλωση, επικοινωνήστε με το αρμόδιο τοπικό γραφείο, την τοπική υπηρεσία διάθεσης οικιακών απορριμμάτων ή το κατάστημα όπου αγοράσατε το προϊόν.

Készülékek magánháztartásban történő selejtezése az Európai Unió területén

A készüléken, illetve a készülék csomagolásán látható azonos szimbólum annak jelzésére szolgál, hogy a készülék a selejtezés során az egyéb háztartási hulladéktól eltérő módon kezelendő. A vásárló a hulladékká vált készüléket köteles a kijelölt gyűjtőhelyre szállítani az elektromos és elektronikai készülékek újrahasznosítása céljából. A hulladékká vált készülékek selejtezéskori begyűjtése és újrahasznosítása hozzájárul a természeti erőforrások megőrzéséhez, valamint biztosítja a selejtezett termékek környezetre és emberi egészségre nézve biztonságos feldolgozását. A begyűjtés pontos helyéről bővebb tájékoztatást a lakhelye szerint illetékes önkormányzattól, az illetékes szemételtakarító vállalattól, illetve a terméket elárusító helyen kaphat.

Smaltimento delle apparecchiature da parte di privati nel territorio dell'Unione Europea

Questo simbolo presente sul prodotto o sulla sua confezione indica che il prodotto non può essere smaltito insieme ai rifiuti domestici. È responsabilità dell'utente smaltire le apparecchiature consegnandole presso un punto di raccolta designato al riciclo e allo smaltimento di apparecchiature elettriche ed elettroniche. La raccolta differenziata e il corretto riciclo delle apparecchiature da smaltire permette di proteggere la salute degli individui e l'ecosistema. Per ulteriori informazioni relative ai punti di raccolta delle apparecchiature, contattare l'ente locale per lo smaltimento dei rifiuti, oppure il negozio presso il quale è stato acquistato il prodotto.

Nolietotu iekārtu iznīcināšanas noteikumi lietotājiem Eiropas Savienības privātajās mājsaimniecībās

Šāds simbols uz izstrādājuma vai uz tā iesaiņojuma norāda, ka šo izstrādājumu nedrīkst izmest kopā ar citiem sadzīves atkritumiem. Jūs atbildat par to, lai nolietotās iekārtas tiktu nodotas speciāli iekārtotos punktos, kas paredzēti izmantoto elektrisko un elektronisko iekārtu savākšanai otrreizējai pārstrādei. Atsevišķa nolietoto iekārtu savākšana un otrreizējā pārstrāde palīdzēs saglabāt dabas resursus un garantēs, ka šīs iekārtas tiks otrreizēji pārstrādātas tādā veidā, lai pasargātu vidi un cilvēku veselību. Lai uzzinātu, kur nolietotās iekārtas var izmest otrreizējai pārstrādei, jāvēršas savas dzīves vietas pašvaldībā, sadzīves atkritumu savākšanas dienestā vai veikalā, kurā izstrādājums tika nopirkts.

Vartotojų iš privačių namų ūkių įrangos atliekų šalinimas Europos Sąjungoje
Šis simbolis ant gaminio arba jo pakuotės rodo, kad šio gaminio šalinti kartu su kitomis namų ūkio atliekomis negalima. Šalintinas įrangos atliekas privalote pristatyti į specialią surinkimo vietą elektros ir elektroninės įrangos atliekoms perdirbti. Atskirai surenkamos ir perdirbamos šalintinos įrangos atliekos padės saugoti gamtinius išteklius ir užtikrinti, kad jos bus perdirbtos tokiu būdu, kuris nekenkia žmonių sveikatai ir aplinkai. Jeigu norite sužinoti daugiau apie tai, kur galima pristatyti perdirbtinas įrangos atliekas, kreipkitės į savo seniūniją, namų ūkio atliekų šalinimo tarnybą arba parduotuvę, kurioje įsigijote gaminį.

Verwijdering van afgedankte apparatuur door privé-gebruikers in de Europese Unie
Dit symbool op het product of de verpakking geeft aan dat dit product niet mag worden gedeponeerd bij het normale huishoudelijke afval. U bent zelf verantwoordelijk voor het inleveren van uw afgedankte apparatuur bij een inzamelingspunt voor het recyclen van oude elektrische en elektronische apparatuur. Door uw oude apparatuur apart aan te bieden en te recyclen, kunnen natuurlijke bronnen worden behouden en kan het materiaal worden hergebruikt op een manier waarmee de volksgezondheid en het milieu worden beschermd. Neem contact op met uw gemeente, het afvalinzamelingsbedrijf of de winkel waar u het product hebt gekocht voor meer informatie over inzamelingspunten waar u oude apparatuur kunt aanbieden voor recycling.

Pozbywanie się zużytego sprzętu przez użytkowników w prywatnych gospodarstwach domowych w Unii Europejskiej
Ten symbol na produkcie lub jego opakowaniu oznacza, że produktu nie wolno wyrzucać do zwykłych pojemników na śmieci. Obowiązkiem użytkownika jest przekazanie zużytego sprzętu do wyznaczonego punktu zbiórki w celu recyklingu odpadów powstałych ze sprzętu elektrycznego i elektronicznego. Osobna zbiórka oraz recykling zużytego sprzętu pomogą w ochronie zasobów naturalnych i zapewnią ponowne wprowadzenie go do obiegu w sposób chroniący zdrowie człowieka i środowisko. Aby uzyskać więcej informacji o tym, gdzie można przekazać zużyty sprzęt do recyklingu, należy się skontaktować z urzędem miasta, zakładem gospodarki odpadami lub sklepem, w którym zakupiono produkt.

Descarte de Lixo Elétrico na Comunidade Européia
Este símbolo encontrado no produto ou na embalagem indica que o produto não deve ser descartado no lixo doméstico comum. É responsabilidade do cliente descartar o material usado (lixo elétrico), encaminhando-o para um ponto de coleta para reciclagem. A coleta e a reciclagem seletivas desse tipo de lixo ajudarão a conservar as reservas naturais; sendo assim, a reciclagem será feita de uma forma segura, protegendo o ambiente e a saúde das pessoas. Para obter mais informações sobre locais que reciclam esse tipo de material, entre em contato com o escritório da HP em sua cidade, com o serviço de coleta de lixo ou com a loja em que o produto foi adquirido.

Likvidácia vyradených zariadení v domácnostiach v Európskej únii
Symbol na výrobku alebo jeho balení označuje, že daný výrobok sa nesmie likvidovať s domovým odpadom. Povinnosťou spotrebiteľa je odovzdať vyradené zariadenie v zbernom mieste, ktoré je určené na recykláciu vyradených elektrických a elektronických zariadení. Separovaný zber a recyklácia vyradených zariadení prispieva k ochrane prírodných zdrojov a zabezpečuje, že recyklácia sa vykonáva spôsobom chrániacim ľudské zdravie a životné prostredie. Informácie o zberných miestach na recykláciu vyradených zariadení vám poskytne miestne zastupiteľstvo, spoločnosť zabezpečujúca odvoz domového odpadu alebo obchod, v ktorom ste si výrobok zakúpili.

Odstranjevanje odslužene opreme uporabnikov v zasebnih gospodinjstvih v Evropski uniji
Ta znak na izdelku ali njegovi embalaži pomeni, da izdelka ne smete odvreči med gospodinjske odpadke. Nasprotno, odsluženo opremo morate predati na zbirališče, pooblaščeno za recikliranje odslužene električne in elektronske opreme. Ločeno zbiranje in recikliranje odslužene opreme prispeva k ohranjanju naravnih virov in zagotavlja recikliranje te opreme na zdravju in okolju neškodljiv način. Za podrobnejše informacije o tem, kam lahko odpeljete odsluženo opremo na recikliranje, se obrnite na pristojni organ, komunalno službo ali trgovino, kjer ste izdelek kupili.

Eliminación de residuos de equipos eléctricos y electrónicos por parte de usuarios particulares en la Unión Europea

Este símbolo en el producto o en su envase indica que no debe eliminarse junto con los desperdicios generales de la casa. Es responsabilidad del usuario eliminar los residuos de este tipo depositándolos en un "punto limpio" para el reciclado de residuos eléctricos y electrónicos. La recogida y el reciclado selectivos de los residuos de aparatos eléctricos en el momento de su eliminación contribuirá a conservar los recursos naturales y a garantizar el reciclado de estos residuos de forma que se proteja el medio ambiente y la salud. Para obtener más información sobre los puntos de recogida de residuos eléctricos y electrónicos para reciclado, póngase en contacto con su ayuntamiento, con el servicio de eliminación de residuos domésticos o con el establecimiento en el que adquirió el producto.

Bortskaffande av avfallsprodukter från användare i privathushåll inom Europeiska Unionen

Om den här symbolen visas på produkten eller förpackningen betyder det att produkten inte får slängas på samma ställe som hushållssopor. I stället är det ditt ansvar att bortskaffa avfallet genom att överlämna det till ett uppsamlingsställe avsett för återvinning av avfall från elektriska och elektroniska produkter. Separat insamling och återvinning av avfallet hjälper till att spara på våra naturresurser och gör att avfallet återvinns på ett sätt som skyddar människors hälsa och miljön. Kontakta ditt lokala kommunkontor, din närmsta återvinningsstation för hushållsavfall eller affären där du köpte produkten för att få mer information om var du kan lämna ditt avfall för återvinning.

B

Console ports

Contents

Overview B-2
MSM710 Console port B-2
MSM730 Console port B-2
MSM750 Console port B-3

Overview

Console port and cable information for the MSM7xx controllers is provided as follows:

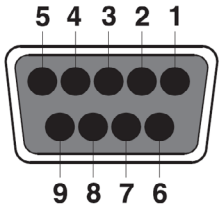
Product	Information to use
MSM710, MSM730, MSM750	Relevant section below
MSM760, MSM765zl	The provided Installation and Getting Started Guide.

MSM710 Console port

The MSM710 provides a DB-9 (female) Console (serial) port connector. The DB-9 connector (DCE) has pin assignments as follows:

Pin	Signal	Direction
1	DCD	→ to PC
2	RXD	→ to PC
3	TXD	← from PC
4	DTR	← from PC
5	GND	
6	DSR	→ to PC
7	RTS	← from PC
8	CTS	→ to PC
9	Unused	

Connector



DB-9 (female)

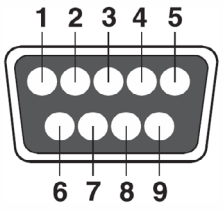
To connect to a computer, use a standard (straight through) serial cable (male-to-female).

MSM730 Console port

The MSM730 provides a DB-9 (male) Console (serial) port connector (DTE). The DB-9 connector has pin assignments as follows:

Pin	Signal	Direction
1	DCD	← from PC
2	RXD	← from PC
3	TXD	→ to PC
4	DTR	→ to PC
5	GND	
6	DSR	← from PC
7	RTS	→ to PC
8	CTS	← from PC
9	Unused	

Connector

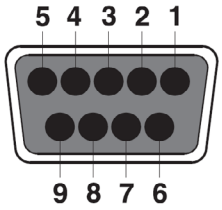


DB-9 (male)

To connect to a computer, use the supplied null-modem serial cable.

MSM750 Console port

The MSM750 provides an RJ-45 Console (serial) port connector. Connect the supplied RJ-45 to DB-9 (female) adapter. The DB-9 connector (DCE) has pin assignments as follows:

Pin	Signal	Direction	Connector
1	DCD	→ to PC	
2	RXD	→ to PC	
3	TXD	← from PC	
4	DTR	← from PC	
5	GND		
6	DSR	→ to PC	
7	RTS	← from PC	
8	CTS	→ to PC	
9	Unused		

DB-9 (female)

To connect to a computer, use a standard (straight through) serial cable (male-to-female).

C

Resetting to factory defaults

Contents

How it works..... C-2
Using the Reset button..... C-2
Using the management tool..... C-2
Using the Console (serial) port..... C-3

How it works

Depending on the service controller model, there may be more than one way to reset the service controller to its factory default settings. This appendix describes the methods available for each model type.

Caution

Resetting a service controller to factory defaults deletes all configuration settings, resets the manager username and password to "admin," disables the DHCP server on the LAN port, sets the LAN port IP address to 192.168.1.1 (MSM765zl LAN port has no factory-default IP address), and sets the Internet port to operate as a DHCP client.

Note

User-installed licenses are retained after a factory reset, but are deactivated. See *Factory reset considerations on page 15-8*.

Using the Reset button

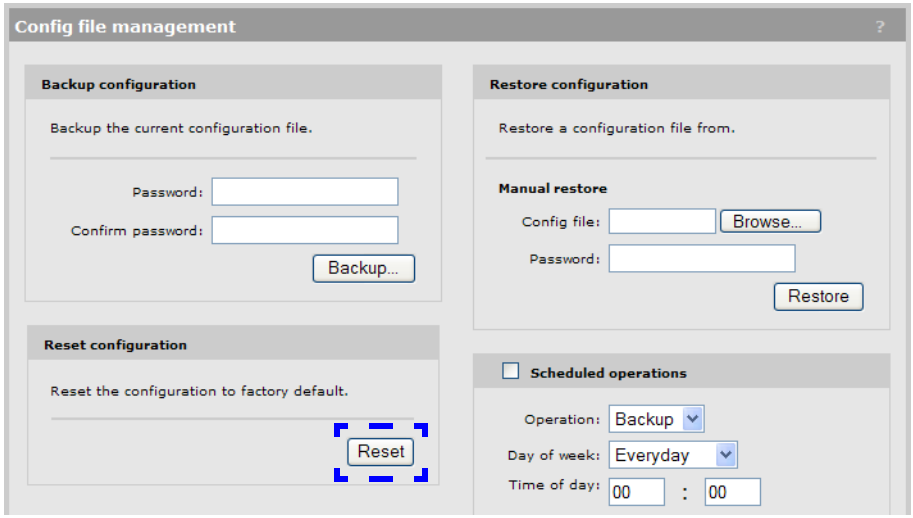
(MSM710 only.)

Using a tool such as a paper clip, press and hold the reset button (back of MSM710) for a few seconds until the front status lights blink three times.

Using the management tool

Supported on models: MSM710, MSM730, MSM750, MSM765zl, MSM760

1. Launch the management tool (default https://192.168.1.1).
2. Select **Service Controller >> Maintenance > Config file management**, and in section **Reset configuration**, select **Reset**.



Using the Console (serial) port

Supported on models: MSM730, MSM750, MSM760

Note

It is recommended that you use the management tool as previously described to reset a service controller to factory defaults. However, if you forgot the manager username or password, you can still force factory reset as described here:

1. Power off the service controller.
2. Connect a serial cable to the service controller console port as follows:
   - For the MSM730, and MSM750, see the relevant section in *Appendix B: Console ports*.
   - For the MSM760, see the *MSM760 Controllers Installation and Getting Started Guide*.
3. Configure a communications terminal program such as Microsoft Hyperterminal for Windows or Minicom for Linux as follows:
   - **Terminal**: VT-100 (ANSI)
   - **Speed**: Set speed according to the service controller model:
     - For the MSM730 and MSM750, set speed to 115200 bps.
     - For the MSM760, set speed to 9600 bps.
   - **Data bits**: 8
   - **Stop bits**: 1
   - **Parity**: none
   - **Flow control**: none
4. Open an appropriately-configured terminal session.
5. Power on the service controller. System boot messages appear.
6. **Do not press any keyboard keys**. Wait for the LILO prompt to appear. It looks like this:

   ```
   LILO 22.1 boot:
   ```

Important

As soon as the LILO prompt appears, tap the keyboard space bar to prevent the automatic (non-factory-default) boot from continuing. You must tap the space bar or other key within four seconds of the prompt appearing.

7. At the LILO prompt, type the command `linux factory` and press **Enter**. The boot with factory defaults begins.

D

NOC authentication

Contents

Main benefits D-2

How it works D-2

Activating a remote login page with NOC authentication D-4

Addressing security concerns D-5
- Securing the remote login page D-5
- Authenticating with the login application D-6
- Authenticating the service controller D-6
- NOC authentication list D-6

Setting up the certificates D-6
- Install certificates on the Web server D-7
- Define attributes D-7
- Install a certificate on service controller D-7

Authenticating users D-8
- Returned values D-9
- Examples of returned HTML code D-11

Simple NOC authentication example D-12

Forcing user logouts D-13

Main benefits

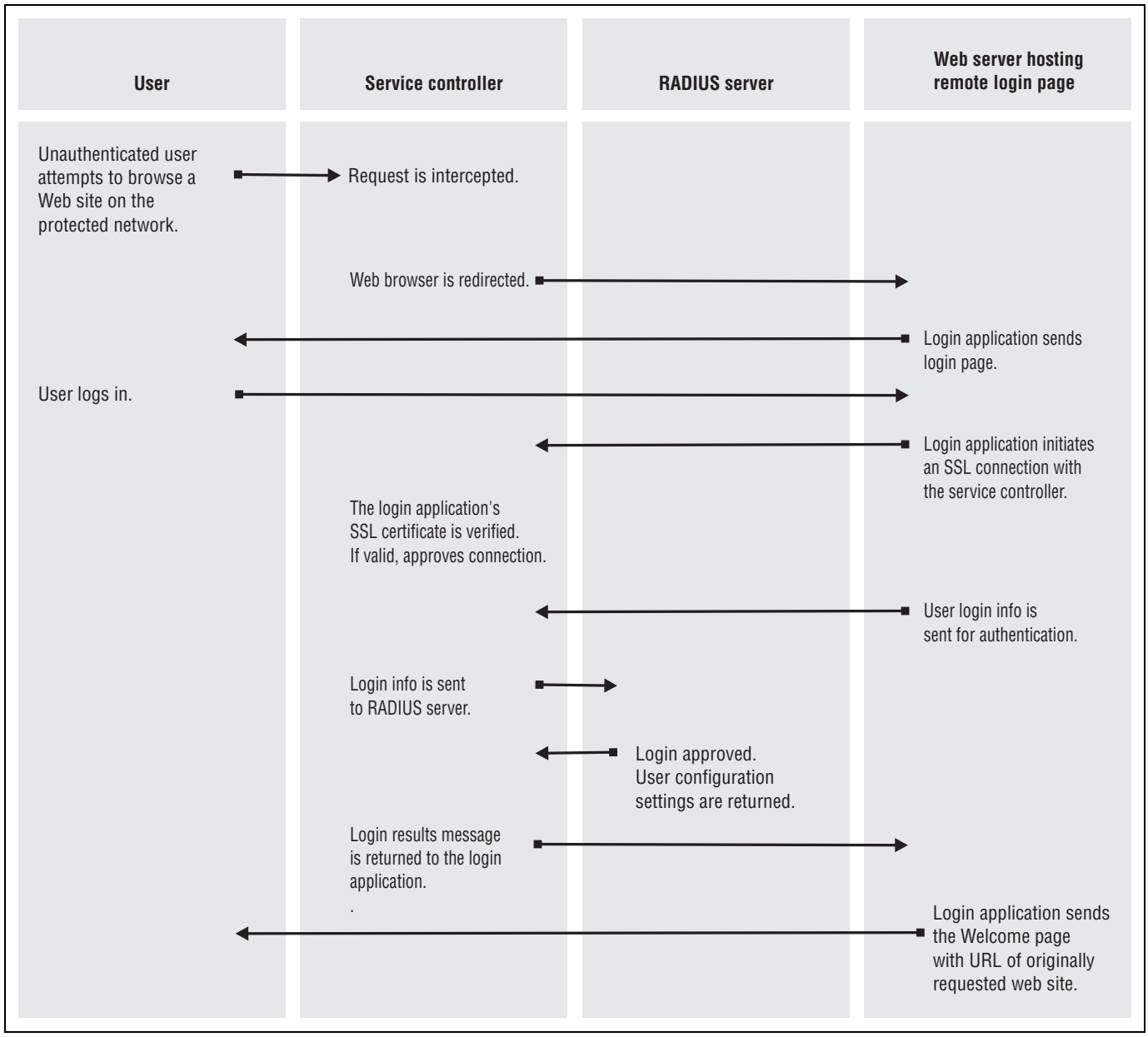
Using a remote login page with NOC (network operations center) authentication provides you with the following benefits:

- The login page is completely customizable. You are not bound by the limits imposed by loading a login page onto the service controller.
- Users can login to the public access interface without exposing their Web browsers to the SSL certificate on the service controller. This eliminates warning messages caused by having an SSL certificate on the service controller that is not signed by a well-known certificate authority.
- If you want to support secure login with SSL, but have multiple service controllers, using a remote login page means you only need to purchase a single SSL certificate signed by a well-known certificate authority, instead of one for each access point.

How it works

The NOC authentication feature provides a secure way of authenticating public access users, with strong mutual authentication between the login application on the Web server hosting the remote login page and the service controller used for authenticating user logins. This occurs via the two Colubris-AVPair value strings (**ssl-noc-certificate** and **ssl-noc-ca-certificate**), which define the locations of two certificates. These certificates enable the service controller to validate that the user login information does indeed come from a trusted application. For example, from a login application on the Web server.

The following diagram shows the sequence of events for a typical user session when using the NOC-based authentication feature.


User
Service controller
RADIUS server
Web server hosting remote login page
Unauthenticated user attempts to browse a Web site on the protected network.
Request is intercepted.
Web browser is redirected.
Login application sends login page.
User logs in.
Login application initiates an SSL connection with the service controller.
The login application's SSL certificate is verified. If valid, approves connection.
User login info is sent for authentication.
Login info is sent to RADIUS server.
Login approved. User configuration settings are returned.
Login results message is returned to the login application.
.
Login application sends the Welcome page with URL of originally requested web site.

Activating a remote login page with NOC authentication

To activate a remote login page, you must define several service controller attributes. These attributes can be defined in the RADIUS account for the service controller (if you are using a RADIUS server) or they can be locally configured.

The following table summarizes the Colubris-AVPair value strings for the remote login page with NOC authentication.

Item	Colubris-AVPair value string
External login	`login-url=`*`URL_of_the_page`* `[`*`placeholder`*`]` URL of the remote login page. Access to the Web server hosting this page must be granted to all unauthenticated users. Do this with an appropriate access list definition.
NOC certificate	`ssl-noc-certificate=`*`URL_of_the_Certificate`* Certificate issued to the application on the Web server that sends user info to the service controller for authentication.
NOC CA certificate	`ssl-noc-ca-certificate=`*`URL_of_the_certificate`* Certificate of the certificate authority (CA) that issued the NOC certificate.
Custom SSL certificate	`ssl-certificate=`*`URL_of_the_certificate`* Custom certificate installed on the service controller.

The following placeholders can be added to the login-url string.

Placeholder	Description
`%c`	Returns the IP address of the user's computer.
`%d`	Returns the WISPr location-ID. Supported for login-url only.
`%e`	Returns the WISPr location-Name. Supported for login-url only.
`%l`	Returns the URL on the service controller where user login information should be posted for authentication. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%n`	Returns the NAS ID assigned to the service controller. By default, this is the unit's serial number. Not supported in local mode.
`%s`	Returns the RADIUS login name assigned to the service controller. By default, this is the unit's serial number. Not supported in local mode.

`%o`	Returns the original URL requested by the user. By default, this value is URL encoded. By default, this value is URL encoded. (To enable/disable URL encoding, set the value of **url-encode** in the **<ACCESS-CONTROLLER>** section in the configuration file.)
`%i`	Returns the domain name assigned to the service controller's Internet port.
`%p`	Returns the port number on the service controller where user login information should be posted to for authentication.
`%a`	Returns the IP address of the service controller's interface that is sending the authentication request.
`%E`	When the location-aware feature is enabled, returns the ESSID of the wireless access point the user is associated with.
`%P`	When the location-aware feature is enabled, returns the wireless mode ("ieee802.11a", "ieee802.11b", "ieee802.11g") the user is using to communicate with the access point.
`%G`	When the location-aware feature is enabled, returns the group name of the wireless access point the user is associated with.
`%C`	When the location-aware feature is enabled, returns the Called-station-id content for the wireless access point the user is associated with.
`%r`	Returns the string sent by the RADIUS server when an authentication request fails. The RADIUS server must be configured to support this feature. The information contained in the returned string depends on the configuration of the RADIUS server.
`%m`	Returns the MAC address of the wireless/wired client station that is being authenticated.
`%v`	Returns the VLAN assigned to the client station at the service controller's ingress (LAN port).

Addressing security concerns

It is important that the connection between the login application and the service controller be secure to protect the exchange of user authentication traffic. The following strategy provides for complete connection security.

Securing the remote login page

HTTPS can be used on the Web server to secure the login page. To avoid warning messages on the user's browser, the SSL certificate installed on the Web server should be signed by a well-known CA.

Authenticating with the login application

The connection between the login application and the service controller is secured using SSL. When establishing the SSL connection with the service controller, the login application must supply its SSL certificate. In a standard SSL setup, the service controller uses the CA for this certificate to validate the certificate's identity and authenticate the login application.

However, the service controller does not want to accept SSL connections from *just any* remote entity with a valid certificate. Rather, it only wants to accept connections from a specific entity: the login application.

To uniquely identify the login application, the *ssl-noc-certificate* attribute is defined in the RADIUS profile for the service controller. This attribute contains the URL of the login application's SSL certificate. When the login application presents its SSL certificate, the service controller retrieves *ssl-noc-certificate* and checks to make sure that they match.

For further authentication, a second attribute, *ssl-noc-ca-certificate*, is defined in the RADIUS profile for the service controller. This attribute contains the URL of the public key of the certificate authority (CA) that signed the login application's SSL certificate. The service controller uses the public key to determine if the login application's SSL certificate can be trusted.

Authenticating the service controller

To identify itself, the service controller uses the SSL certificate configured on the **Security > Certificate Stores** page or via the *ssl-certificate* attribute.

For added security, the login application could also check that this SSL certificate has been signed by the certificate authority for which the login application has the public key certificate. The default certificate installed on the service controller, is not signed by a well-known CA and cannot be used for this purpose. Instead, a new certificate must be installed on the service controller. This certificate could be signed by a well-known certificate authority or your own CA.

NOC authentication list

Additional security is provided via the Security list on the **Public access > Web server** page. You use this list to define the set of remote IP addresses that the service controller accepts authentication requests from. If a request is received from an address not in this list, it is discarded.

Setting up the certificates

This section presents an overview of the certificates you need to install to secure communication between the remote login page and the service controller. For detailed discussion of the issues, see *Addressing security concerns on page D-5*.

Install certificates on the Web server

Install an SSL certificate and its matching CA certificate into a folder on the Web server hosting the remote login page. The login application and the service controller access the certificates from this location.

The SSL certificate is used by the login application to secure communications with the service controller.

Define attributes

Add the following attributes to the **Configured attributes** table on the **Public access > Attributes** page. (You can also define these attributes in the RADIUS profile for the service controller if you are using a RADIUS server.) This enables it to retrieve the SSL and CA certificates from the Web server:

`ssl-noc-certificate=`*`URL_of_the_Certificate`* Certificate issued to the application on the Web server that sends user info to the service controller for authentication.
`ssl-noc-ca-certificate=`*`URL_of_the_certificate`* Certificate of the certificate authority (CA) that issued the NOC certificate.
`ssl-certificate=`*`URL_of_the_certificate`* Custom certificate installed on the service controller.

Install a certificate on service controller

Note

This step is optional, but recommended.

Install an SSL certificate on the service controller to replace its default SSL certificate. This certificate is used to secure communications between the service controller and the login application on the Web server.

If you do not change the default certificate on the service controller, the login application may not be able to validate the service controllers certificate when establishing the SSL connection. The reason for this is because the default certificate is self-signed and is not trusted by any well-known CA.

This can be done by adding an additional attribute to the **Configured attributes** table on the **Public access > Attributes** page. (You can also define this attribute in the RADIUS profile for the service controller if you are using a RADIUS server.).

`ssl-certificate=`*`URL_of_the_certificate`*

Authenticating users

After a user has supplied login information on the remote login page, the login application must submit an authentication request containing the user's login name, password, and IP address to the service controller by establishing an SSL session to the following URL:

```
https://service controller_ip:8090/goform/HtmlNocLoginRequest
?username=username&password=password&ipaddr=user_ip
```

Where:

Parameter	Description
`service controller_ip`	Defines the IP address of the service controller or you could use a domain name if you have defined one using the hosts file on the Web server. (By default, the secure Web server on the service controller operates on port 8090. This can be changed on the **Management > Management Tool** page if required.) The service controller requires that the contents of the Host HTTP header match the actual domain name/IP address and port the service controller is operating on: Host: service controller_domain_name:secure_web_server_port_number or Host: service controller_IP_address:secure_web_server_port_number This is usually the case unless the service controller is behind a device that provides network address translation (NAT). In this situation, the login application must manually forge the Host HTTP header. The easiest way to do this is to define `login-url` with the `%i` and `%p` placeholders. This returns the domain name of the service controller and the port number of its secure Web server. The login application can then construct the appropriate Host HTTP header.
`username`	Username supplied by the user.
`password`	Password supplied by the user.
`user_ip`	IP address of the user's computer.

Example 1

Assume that the service controller is not behind a NATing device, and that its IP address is 192.168.4.2. The subject DN in its SSL certificates is www.noc-cn3.com.

The Host HTTP header should be set to one of:

- Host: www.noc-cn3.com:8090
- Host: 192.168.4.2:8090

Example 2

Assume that the service controller is behind a NATting device. The device has the address 192.168.30.173, and the service controller has the address 192.168.4.2. A NAT mapping is defined on the NATting device that redirects traffic received on port 8090 to 192.168.4.2:8090.

The login application must send its requests to 192.168.30.173, which results in a HTTP Host header that contains one of the following:

- Host: natting.device.com:8090
- Host: 192.168.30.173:8090

When this request is forwarded to the service controller, it is rejected. To solve the problem, the login application must forge the host HTTP header. This is easily done by plugging in the values returned by the %i, %a, and %p placeholders. For example:

Host: %i:%p
or
Host: %a,%p

The service controller sends the username and password to the RADIUS server to authenticate the user. If authentication is successful, the user's IP address is used to grant wireless network access to the user's computer.

The service controller returns a positive or negative answer for the user login, along with the relevant URLs that may be needed by the login application in order to redirect the user to either a Welcome page or a Login error page located on the Web server. This information is returned as standard HTML. The login application must parse this information to retrieve the response. All possible responses are described in the following section.

Returned values

The following examples show the information returned for various authentication conditions.

NOC authentication mode is not enabled

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_DISABLED
</HTML>
```

The service controller did not receive the login application's SSL certificate

The login application did not send its certificate. Therefore, the request was rejected.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CANNOT_GET_PEER_CERT
</HTML>
```

Certificate mismatch

The login application sent an SSL certificate that does not match the one defined by ssl-noc-certificate in the RADIUS profile for the service controller.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CANNOT_GET_PEER_CERT
</HTML>
```

Certificate not valid yet

The login application sent an SSL certificate that matches the one defined by ssl-noc-certificate in the RADIUS profile for the service controller. However, the certificate that was sent is not yet valid.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CERT_NOT_YET_VALID
</HTML>
```

Certificate not valid anymore

The login application sent an SSL certificate that matches the one defined by ssl-noc-certificate in the RADIUS profile for the service controller. However, the certificate that was sent is not valid anymore.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CERT_EXPIRED
</HTML>
```

Certificate not signed by proper CA

The login application sent a valid SSL certificate that matches the one defined by ssl-noc-certificate in the RADIUS profile for the service controller. However, the certificate is not signed by the CA defined by noc-ca-certificate in the RADIUS profile for the service controller.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_CERT_NOT_SIGNED_BY_AUTHORIZED_CA
</HTML>
```

Missing username and/or password

The user's username or password was not supplied.

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=NOC_MISSING_USERNAME_OR_PASSWORD
</HTML>
```

The specified IP address is already logged in

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_LOGGED_IN
</HTML>
```

Authentication was successful

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_SUCCESS
NOC_INFO_WELCOME_URL=<welcome url>
NOC_INFO_SESSION_URL=<session url>
</HTML>
```

Authentication failed

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_ERR_MESSAGE=<error message>
NOC_INFO_LOGIN_ERR_URL =<login error url>
</HTML>
```

Logout succeeded

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_SUCCESS
</HTML>
```

Logout failed

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=<error message>
</HTML>
```

Examples of returned HTML code

The following examples show the actual HTML code returned file for various authentication conditions.

User was successfully authenticated by the RADIUS server

```
<HTML>
status=success
welcome-url=https://206.162.167.226:8888/cebit-php/
welcome.php?site=www.noc-service
controller.com&user=user00&wantedurl=&nasipaddress=&nasid=L003-00069
session-url=http://192.168.1.1:8080/session.asp
</HTML>
```

User's IP address is already in use by an active session

```
<HTML>
status=already-logged-in
</HTML>
```

User authentication was refused by the RADIUS server

This could be due to an unknown username, or invalid username or password.

```
<HTML>
status=failure
external-err-msg=Your login was refused.
login-err-url=https://206.162.167.226:8888/cebit-php/login-
error.php?site=john-cn3000&user=user12&nasipaddress=
</HTML>
```

User could not be authenticated

The service controller could not contact a RADIUS server.

```
<HTML>
status=failure
external-err-msg=You cannot be logged in at this time. Please try again
later.
login-err-url=https://206.162.167.226:8888/cebit-php/login-
error.php?site=john
-cn3000&user=user12&nasipaddress=
</HTML>
```

Simple NOC authentication example

This is a simple example showing how to use the NOC authentication feature.

1. Create the following folder on your Web sever: **newlogin.**
2. See *Public access examples on page 8-4*. Copy the following example files into the **newlogin** folder:
   - login.html
   - transport.html
   - session.html
   - fail.html
   - logo.gif
3. Customize **login.html** to accept username and password information from users and then send it to the service controller. You could use code similar to the following PHP example to send login information back to the service controller for authentication:

   ```
   https://ipaddress of CNx:8090/goform/HtmlNocLoginRequest
   ?username=username&password=password&ipaddress=user_ip
   ```

   The variable `loginurl` contains the URL on the service controller where user information is sent for authentication.
4. Start the management tool.
5. Click **Public access** > **Web server**.

6. Enable the **NOC-based authentication** feature.
7. Under **Security** add the IP address of the Web server to the **Allowed Addresses** box.
8. Under **Active interfaces** make sure that the interface on which the request will be received is enabled.
9. Click **Save**.
10. Add the following entries to the **Configured attributes** table on the **Public access > Attributes** page. (You can also define these attributes in the RADIUS profile for the service controller if you are using a RADIUS server.)

    `login-url=`*`URL_of_page_on_remote_server`*

    `access-list=loginserver,ACCEPT,tcp,`*`web_server_IP_address`*`,443`

    `ssl-noc-certificate=`*`URL_of_the_certificate`*

    `ssl-noc-ca-certificate=`*`URL_of_the_certificate`*

    `transport-page=`*`web_server_URL`*`/newlogin/transport.html`

    `session-page=`*`web_server_URL`*`/newlogin/session.html`

    `fail-page=`*`web_server_URL`*`/newlogin/fail.html`

    `logo=`*`web_server_URL`*`/newlogin/logo.gif`

    `use-access-list=loginserver`

Forcing user logouts

Users can be logged out by calling the following URL:

```
https://service controller_ip:8090/goform/HtmlNocLogoutRequest
?ipaddress=user_ip
```

Note

This request must come from the login application (or another other application that is using the same SSL certificate).

The service controller returns a positive or negative answer for the user logout as standard HTML. The login application must parse this information to retrieve the response.

Logout success

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_SUCCESS
</HTML>
```

Logout failure

```
<HTML>
NOC_INFO_STATUS=NOC_STATUS_FAILURE
NOC_INFO_INT_ERR_MESSAGE=<error message>
</HTML>
```

These definitions are contained in **noc.h**.

E

DHCP servers and Colubris vendor classes

Contents

Overview E-2

Windows Server 2003 configuration E-2

ISC DHCP server configuration E-7

Overview

This section shows you how to configure the following DHCP servers to use the vendor-specific class:

- *Windows Server 2003 configuration on page E-2.*
- *ISC DHCP server configuration on page E-7.*

A vendor class allows certain devices to request specific information from a Dynamic Host Configuration Protocol server. Specifically, the HP ProCurve vendor class enables you to define a list of available service controllers to which APs operating in controlled mode can connect.

When DHCP clients send the Colubris *vendor class identifier* in a DHCP request, a properly configured DHCP server returns the Colubris-specific options defined on the server. These values are returned as DHCP option 43 (vendor-specific information) and can be interpreted only by a HP ProCurve device.

Windows Server 2003 configuration

This section describes how to configure a Windows 2003 DHCP server to use the HP ProCurve vendor class.

The following procedure assumes that you have a Windows 2003 Server that has a DHCP server configured and running.

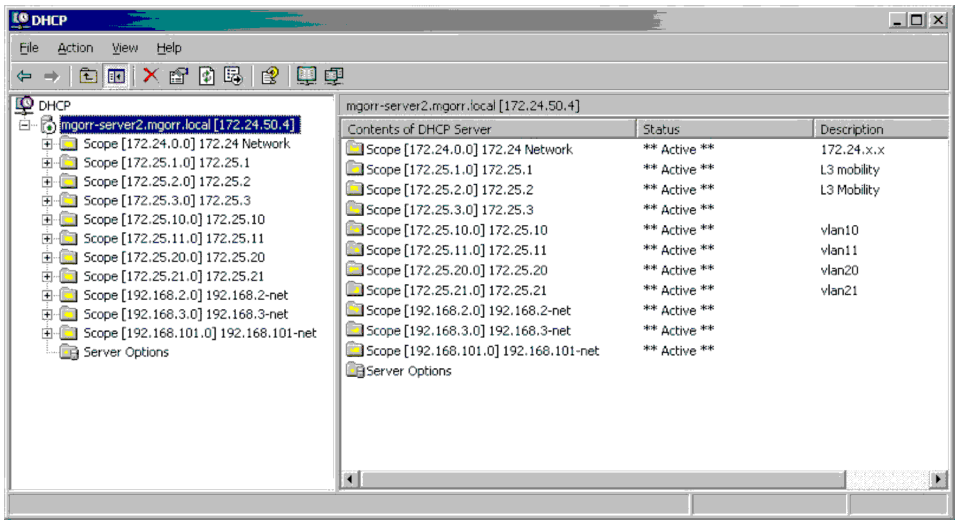
For more information see “Configuring Options and Classes on Windows Server” at

http://technet2.microsoft.com/WindowsServer/en/Library/d55609a5-2a1c-4f3f-ba8f-42b21828dc201033.mspx

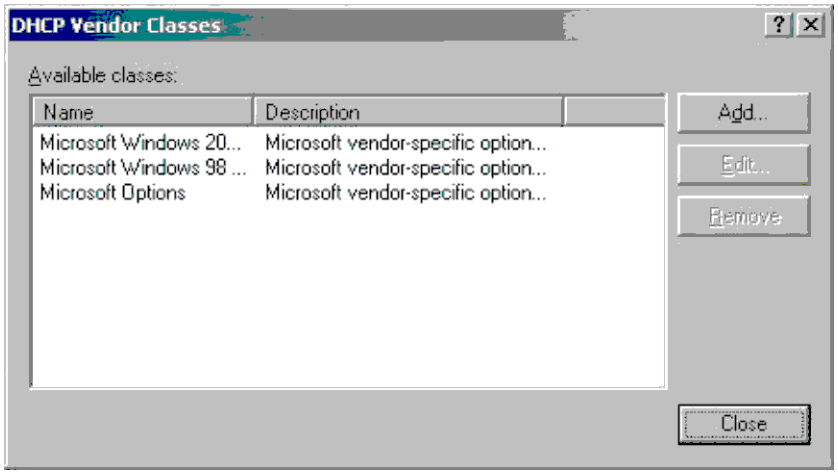
Creating the vendor class

Use the following steps to create the Colubris vendor class on the DHCP server.

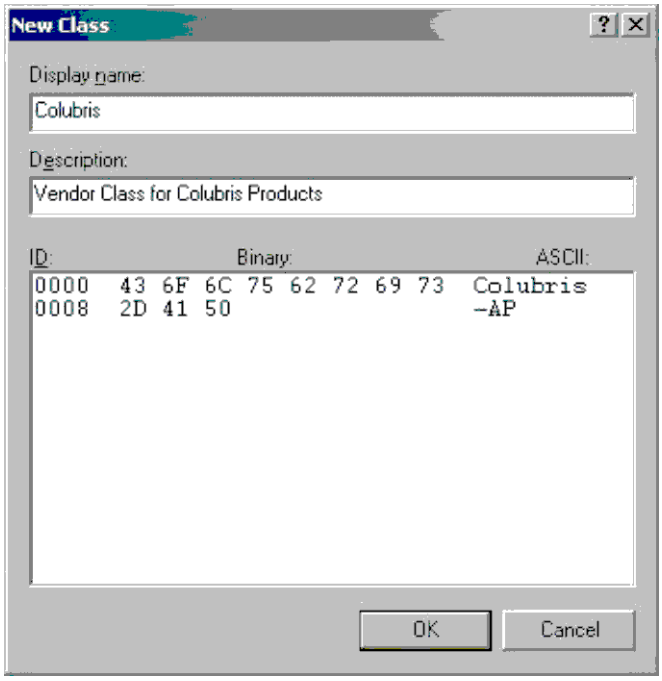
1. Select **Start > Settings > Control Panel > Administrative Tools > DHCP.** The **DHCP** administration page opens.


DHCP
File Action View Help
DHCP
mgorr-server2.mgorr.local [172.24.50.4]
Scope [172.24.0.0] 172.24 Network
Scope [172.25.1.0] 172.25.1
Scope [172.25.2.0] 172.25.2
Scope [172.25.3.0] 172.25.3
Scope [172.25.10.0] 172.25.10
Scope [172.25.11.0] 172.25.11
Scope [172.25.20.0] 172.25.20
Scope [172.25.21.0] 172.25.21
Scope [192.168.2.0] 192.168.2-net
Scope [192.168.3.0] 192.168.3-net
Scope [192.168.101.0] 192.168.101-net
Server Options
mgorr-server2.mgorr.local [172.24.50.4]
Contents of DHCP Server
Status
Description
Scope [172.24.0.0] 172.24 Network ** Active ** 172.24.x.x
Scope [172.25.1.0] 172.25.1 ** Active ** L3 mobility
Scope [172.25.2.0] 172.25.2 ** Active ** L3 Mobility
Scope [172.25.3.0] 172.25.3 ** Active **
Scope [172.25.10.0] 172.25.10 ** Active ** vlan10
Scope [172.25.11.0] 172.25.11 ** Active ** vlan11
Scope [172.25.20.0] 172.25.20 ** Active ** vlan20
Scope [172.25.21.0] 172.25.21 ** Active ** vlan21
Scope [192.168.2.0] 192.168.2-net ** Active **
Scope [192.168.3.0] 192.168.3-net ** Active **
Scope [192.168.101.0] 192.168.101-net ** Active **
Server Options

2. On the **DHCP** administration page in the navigation pane at left, select the name of the DHCP server to manage, and then select **Action > Define Vendor Classes.** The **DHCP Vendor Classes** page opens. Several default Microsoft vendor classes are preconfigured.



3. On the **DHCP Vendor Classes** page, select **Add.** The **New Class** page opens.

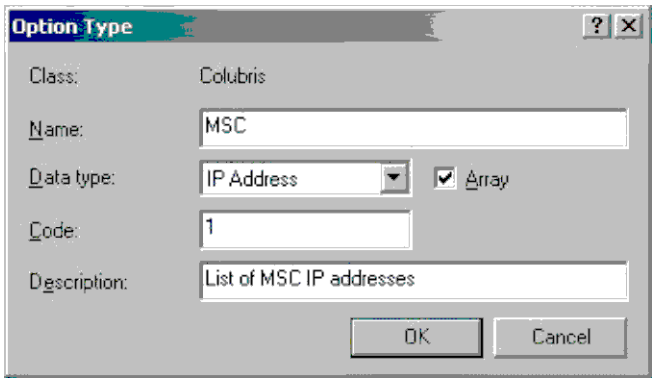


4. On the **New Class** page
   - Under **Display name,** specify **Colubris.**
   - Under **Description,** specify any desired descriptive information for this vendor class.
   - Select under **ASCII** and specify **Colubris-AP.**
   - Select **OK.**
5. The **New Class** page closes, and you return to the **DHCP Vendor Classes** page. To close the **DHCP Vendor Classes** page and return to the **DHCP** administration page, select **Close.**

Defining vendor class options

Use the following steps to define Colubris vendor class options on the DHCP server.

1. On the **DHCP** administration page, select **Action > Set Predefined Options.** From the **Option class** drop-down menu, select **Colubris,** and then select **Add.** The **Option Type** page opens.



2. On the **Option Type** page,
   - Under **Name,** specify **MSC** (for MSM controllers).
   - Under **Data type,** select **IP Address** and enable the **Array** checkbox.
   - Under **Code,** specify **1.**
   - Under **Description,** specify **List of MSC IP addresses** (for MSM controller IP addresses).
3. Select **OK** to close the **Option Type** page, and then select **OK** again to return to the **DHCP** administration page.

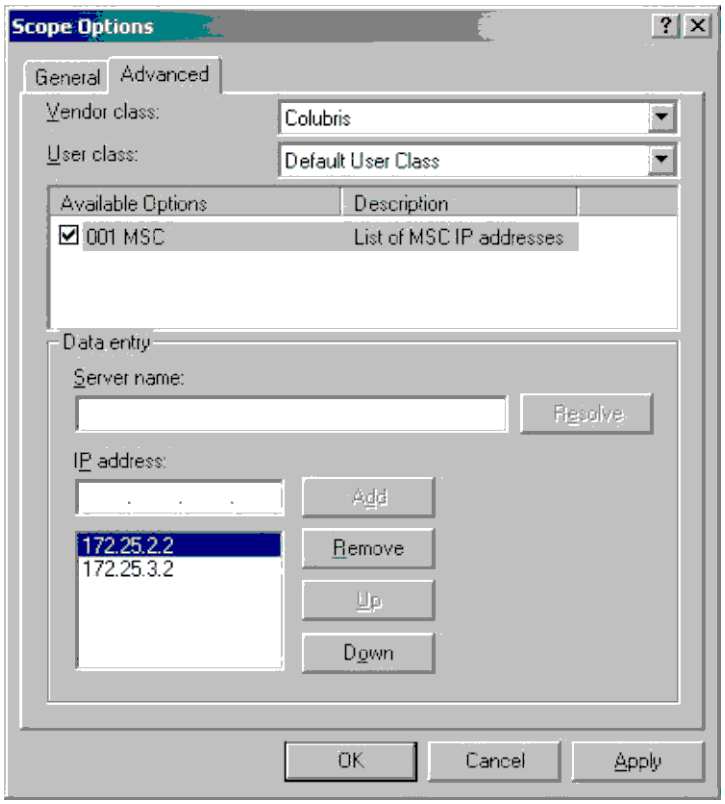
Applying the vendor class

After you define the Colubris vendor class and its options, you can apply the class to specific Scopes or to the entire DHCP server. You must define the Colubris vendor class for every Scope from which an AP can get an address.

Use the following steps to add the Colubris vendor-specific option to one **Scope** on the DHCP server.

1. On the **DHCP** administration page, in the navigation pane, open the folder that corresponds to the desired **Scope**.

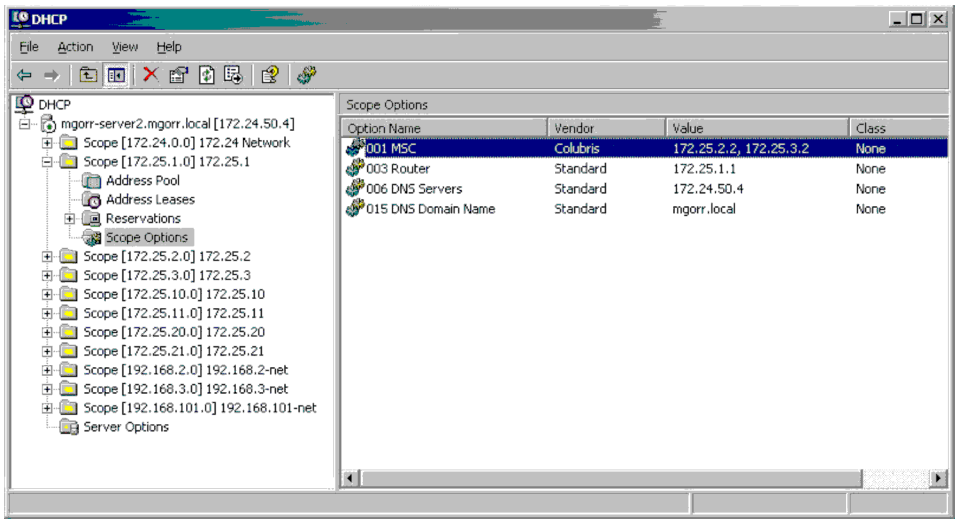
2. Right-click **Scope Options,** and from the resulting menu select **Configure Options.** The **Scope Options** page opens. Select the **Advanced** tab.



3. On the **Advanced** tab, configure the following:

   - From the **Vendor class** drop-down menu, select **Colubris.**
   - Under **Available options,** enable the **001 MSC** checkbox.
   - Under **IP address,** specify the IP address of the primary service controller in your network and select **Add.** Continue to build a list by specifying the IP addresses of all service controllers in your network, in descending order of importance.
   - Select **OK**.

4. The service controller IP addresses now appear on the DHCP administration page under **Scope Options.** When an AP requests an IP address, these addresses are returned in a DHCP Ack message as option 43.



Note For information on solving problems, see *Troubleshooting on page E-9*.

ISC DHCP server configuration

This section shows you how to configure a Linux machine running an Internet Systems Consortium (ISC) DHCP server to use the Colubris Networks vendor class. The procedure assumes that you have a Linux or Unix server that is running the ISC DHCP server.

You configure the ISC DHCP server by editing its configuration file; specifically, the main configuration file, */etc/dhcpd.conf*.

Following is a simple example of the */etc/dhcpd.conf* configuration file:

```
# dhcpd.conf
ddns-update-style ad-hoc;
option domain-name "colubris.com";
option domain-name-servers 172.25.1.3;
default-lease-time 3600;

subnet 172.25.1.0 netmask 255.255.255.0 {
        range 172.25.1.100 172.25.1.150;
        option routers 172.25.1.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.1.255;

}
subnet 172.25.2.0 netmask 255.255.255.0 {
        range 172.25.2.100 172.25.2.150;
        option routers 172.25.2.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.2.255;
}
```

This sample file defines some general options to apply to all clients, as well as two DHCP Scopes—172.25.1.x and 172.25.2.x. You must add lines to the *dhcpd.conf* file to define the following for the ISC server:

- What the Colubris vendor class identifier looks like
- What to return to the client when it sees that identifier.

The following explains the changes that you must make to this sample file and the function of each added line.

- Create an option space called **Colubris** and define a variable called **msc-address** within the space by adding the following lines.

  ```
  option space Colubris;

  option Colubris.msc-address code 1 = array of ip-address;
  ```

- Tell the server what to do when the client sends the vendor class identifier **Colubris-AP** by adding the following lines. In this case you want the server to return the options defined in the Colubris space that was created in the first step. Using the **vendor-option-space** command tells the server to return these values using DHCP option 43.

  ```
  if option vendor-class-identifier =  "Colubris-AP" {

          vendor-option-space Colubris;

  }
  ```

- Specify the service controller IP addresses to return to the client by adding the following lines, where **172.25.2.2** and **172.25.3.2** are the specific IP addresses that you want returned. You can define this option globally or in one or more Scopes. You must define this option on all subnets from which an AP can potentially get an IP address. In this example only clients on the 172.25.1.x subnet get this option.

  ```
  option Colubris.msc-address 172.25.2.2, 172.25.3.2;
  ```

Following is a revised sample configuration file that contains these additions, which appear in bold:

```
# dhcpd.conf
ddns-update-style ad-hoc;
option domain-name "colubris.com";
option domain-name-servers 172.25.1.3;
default-lease-time 3600;

option space Colubris;
option Colubris.msc-address code 1 = array of ip-address;

if option vendor-class-identifier =  "Colubris-AP" {
        vendor-option-space Colubris;
}


subnet 172.25.1.0 netmask 255.255.255.0 {
        range 172.25.1.100 172.25.1.150;
        option routers 172.25.1.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.1.255;
        option Colubris.msc-address 172.25.2.2, 172.25.3.2;
```

```
}

subnet 172.25.2.0 netmask 255.255.255.0 {
        range 172.25.2.100 172.25.2.150;
        option routers 172.25.2.1;
        option subnet-mask 255.255.255.0;
        option broadcast-address 172.25.2.255;
}
```

Troubleshooting

This section shows an Ethereal trace of a DHCP transaction, with the frames edited for readability. Four frames must be exchanged between the client and the server:

1. Client sends a `DHCP-Discover`.
2. Server sends a `DHCP-Offer`.
3. Client sends a `DHCP-Request`.
4. Server sends a `DHCP-Ack`.

The client sends its vendor class identifier in the `DHCP-Request` frame. The DHCP field of Frame 3 is expanded below.

The server sends the service controller addresses encapsulated as option 43 in the `DHCP-Ack` frame. Unfortunately, the only way to decode these values is to look at the hexadecimal data. In this case the server returned the following 10 bytes:

```
2b 0a 01 08 ac 19 02  02 ac 19 03 02
```

which can be decoded as shown in the following table.

Segment	Value	Meaning
2b	43	DHCP option 43
0a	10	Field is 10 bytes long
01	01	Colubris option code 1 as defined in the DHCP server
08	08	Option code 1 is 8 bytes long
ac 19 02 02	172.25.2.2	Service controller IP addresses to return to the client
ac 19 03 02	172.25.3.2	

```
Frame 1 - DHCP-Discover

Frame 1 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Colubris_01:5f:05 (00:03:52:01:5f:05), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
```

```
Frame 2 - DHCP-Offer

Frame 2 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Cisco_23:0e:80 (00:0d:bc:23:0e:80), Dst: Colubris_01:5f:05
(00:03:52:01:5f:05)
802.1Q Virtual LAN
Internet Protocol, Src: 172.25.1.1 (172.25.1.1), Dst: 172.25.1.201 (172.25.1.201)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol

Frame 3 - DHCP-Request

Frame 3 (346 bytes on wire, 346 bytes captured)
Ethernet II, Src: Colubris_01:5f:05 (00:03:52:01:5f:05), Dst: Broadcast
(ff:ff:ff:ff:ff:ff)
802.1Q Virtual LAN
Internet Protocol, Src: 0.0.0.0 (0.0.0.0), Dst: 255.255.255.255 (255.255.255.255)
User Datagram Protocol, Src Port: bootpc (68), Dst Port: bootps (67)
Bootstrap Protocol
    Message type: Boot Request (1)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4262bc18
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 0.0.0.0 (0.0.0.0)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 0.0.0.0 (0.0.0.0)
    Client MAC address: Colubris_01:5f:05 (00:03:52:01:5f:05)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP Request
    Option 54: Server Identifier = 172.24.50.4
    Option 50: Requested IP Address = 172.25.1.201
    Option 60: Vendor class identifier = "Colubris-AP"
    Option 12: Host Name = "R054-00118"
    Option 55: Parameter Request List
    End Option
    Padding


Frame 4 - DHCP-Ack

Frame 4 (358 bytes on wire, 358 bytes captured)
Ethernet II, Src: Cisco_23:0e:80 (00:0d:bc:23:0e:80), Dst: Colubris_01:5f:05
(00:03:52:01:5f:05)
802.1Q Virtual LAN
Internet Protocol, Src: 172.25.1.1 (172.25.1.1), Dst: 172.25.1.201 (172.25.1.201)
User Datagram Protocol, Src Port: bootps (67), Dst Port: bootpc (68)
Bootstrap Protocol
    Message type: Boot Reply (2)
    Hardware type: Ethernet
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x4262bc18
    Seconds elapsed: 0
    Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0 (0.0.0.0)
    Your (client) IP address: 172.25.1.201 (172.25.1.201)
    Next server IP address: 0.0.0.0 (0.0.0.0)
    Relay agent IP address: 172.25.1.1 (172.25.1.1)
```

```
    Client MAC address: Colubris_01:5f:05 (00:03:52:01:5f:05)
    Server host name not given
    Boot file name not given
    Magic cookie: (OK)
    Option 53: DHCP Message Type = DHCP ACK
    Option 58: Renewal Time Value = 12 hours
    Option 59: Rebinding Time Value = 21 hours
    Option 51: IP Address Lease Time = 1 day
    Option 54: Server Identifier = 172.24.50.4
    Option 1: Subnet Mask = 255.255.255.0
    Option 3: Router = 172.25.1.1
    Option 15: Domain Name = "mgorr.local"
    Option 6: Domain Name Server = 172.24.50.4
    Option 43: Vendor-Specific Information (10 bytes)
    End Option

0000  00 03 52 01 5f 05 00 0d bc 23 0e 80 81 00 00 65   ..R._....#.....e
0010  08 00 45 00 01 54 81 68 00 00 ff 11 de 33 ac 19   ..E..T.h.....3..
0020  01 01 ac 19 01 c9 00 43 00 44 01 40 68 ec 02 01   .......C.D.@h...
0030  06 00 42 62 bc 18 00 00 00 00 00 00 00 00 ac 19   ..Bb............
0040  01 c9 00 00 00 00 ac 19 01 01 00 03 52 01 5f 05   ............R._.
0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0090  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00a0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00b0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00c0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00d0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00e0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00f0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0100  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0110  00 00 00 00 00 00 00 00 00 00 63 82 53 63 35 01   ..........c.Sc5.
0120  05 3a 04 00 00 a8 c0 3b 04 00 01 27 50 33 04 00   .:.....;...'P3..
0130  01 51 80 36 04 ac 18 32 04 01 04 ff ff ff 00 03   .Q.6...2........
0140  04 ac 19 01 01 0f 0c 6d 67 6f 72 72 2e 6c 6f 63   .......mgorr.loc
0150  61 6c 00 06 04 ac 18 32 04 2b 0a 01 08 ac 19 02   al.....2.+......
0160  02 ac 19 03 02 ff                                 ......
```

Technology for better business outcomes

To learn more, visit www.hp.com/go/procurve/

© Copyright 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP will not be liable for technical or editorial errors or omissions contained herein.

May 2009

Manual Part Number
5992-5929